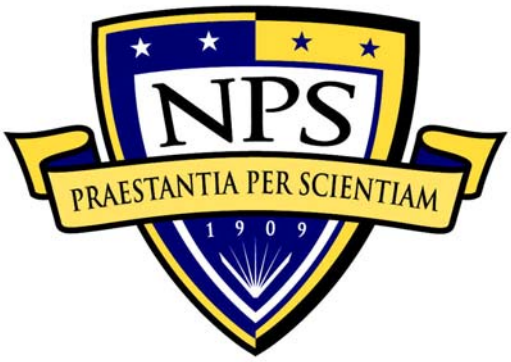

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROBABLE SUCCESS: RISK COMMUNICATION AND THE TERRORISM HAZARD

by

Anthony A. Cox

March 2010

Thesis Advisor:	Lauren F. Wollman
Second Reader:	Ellen M. Gordon

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2010	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Improbable Success: Risk Communication and the Terrorism Hazard	
6. AUTHOR(S) Anthony A. Cox	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. **IRB number NA**

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

This research considers whether America's efforts to warn the public of terrorism can be improved by utilizing risk communication principles with the Homeland Security Advisory System (HSAS), or if not, how the Department of Homeland Security (DHS) should handle risk communication in the future. The research proceeds from the assumption that the HSAS is irreparably flawed, due to specific public communication issues unique to terrorism.

This research uses a policy analysis method to establish a better understanding of the impact and implications of the HSAS on homeland security. Existing literature on this subject is either abundant for hazards other than terrorism or minimal and watered down when terrorism is grouped with "all-hazards." Unforeseen future changes in technology, politics, and society will require continued review of this subject matter and related policy; it is anticipated that this research will help those future efforts.

There is no evidence that the American public can be provided with more than vague and general information regarding threats of terrorism and the specificity required by risk communication principles is better used to support prevention efforts. Recommendations for future homeland security risk communication policy address the formation and sustainment of public resiliency through education.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Advisory system, education, homeland security, intelligence, politics, psychology, public warning, risk communication, sociology, technology, terrorism.	79
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPROBABLE SUCCESS: RISK COMMUNICATION AND THE TERRORISM HAZARD

Anthony A. Cox
Individual Assistance Program Manager, Arizona Division of Emergency Management, Phoenix, Arizona
B.S., Arizona State University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS, SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: Anthony A. Cox

Approved by: Lauren F. Wollman
Thesis Advisor

Ellen M. Gordon
Second Reader

Harold A. Trinkunas, PhD
Chairman Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research considers whether America's efforts to warn the public of terrorism can be improved by utilizing risk communication principles with the Homeland Security Advisory System (HSAS), or if not, how the Department of Homeland Security (DHS) should handle risk communication in the future. The research proceeds from the assumption that the HSAS is irreparably flawed, due to specific public communication issues unique to terrorism.

This research uses a policy analysis method to establish a better understanding of the impact and implications of the HSAS on homeland security. Existing literature on this subject is either abundant for hazards other than terrorism or minimal and watered down when terrorism is grouped with "all-hazards." Unforeseen future changes in technology, politics, and society will require continued review of this subject matter and related policy; it is anticipated that this research will help those future efforts.

There is no evidence that the American public can be provided with more than vague and general information regarding threats of terrorism and the specificity required by risk communication principles is better used to support prevention efforts. Recommendations for future homeland security risk communication policy address the formation and sustainment of public resiliency through education.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CAP	Common Alerting Protocol
CIA	Central Intelligence Agency
CMAS	Commercial Mobile Alert System
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CRS	Congressional Research Service
DEAS	Digital EAS
DHNS	Deaf and Hard of Hearing Notification System
DHS	United States Department of Homeland Security
DOD	United States Department of Defense
EAS	Emergency Alert System
ETN	Emergency Telephone Notification
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
GTAS	Geo-Targeted Alerting System
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
IPAWS	Integrated Public Alert and Warning System
JTTF	Joint Terrorism Task Force
MARSEC	Maritime Security Threat System
NCMEC	National Center for Missing & Exploited Children
NCTC	National Counter-Terrorist Center
NLETS	National Law Enforcement Telecommunications System
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
PL	Public Law
SECC	State Emergency Communications Committees
TOPOFF	Top Officials Exercise
TSA	Transportation Security Administration
US	United States
WARN	Web Alert Relay Network
WMD	Weapon of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

My success is dependent upon the support of others. I would like to thank the Arizona Division of Emergency Management for sponsoring my participation in this program. I acknowledge and thank Chris Bellavita and Heather Issvoran for bringing me back, never giving up on me, and believing in my ability. I am grateful to and recognize my committee. My advisor, Lauren Wollman, gave me valuable guidance and mentoring throughout. Ellen Gordon, my second reader, kept me informed of current affairs and found the time to provide input. I thank my editor, Aimee Anderson, for fine-tuning my writing and delivering me to the finish line with a quality product. Above all else, I am grateful for my family. I could not have gotten here without the support of my wife, Audrey, and her unending understanding of the challenges and requirements this program brings. I thank my amazing children, Hannah, Hailey, and Hayden, for always having hugs and love for me at the airport. I thank my mom and dad, Susan and Larry Cox, for their constant support and motivation to better myself and the world around me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Terrorism threat advisories, as we know them today, are a result of the terrorist attacks on September 11, 2001. The Homeland Security Advisory System (HSAS), a color-coded chart of five threat levels, was created and established in 2002 by President George W. Bush through Homeland Security Presidential Directive 3 (HSPD-3). The HSAS was established to set a wide-ranging and effective way to disseminate to all levels of government—authority, the private sector, and to the American people—information regarding the risk of terrorist attacks. The HSAS is applied directly to the federal executive branch and directs all nonmilitary federal agencies to ensure that their operations are consistent with the HSAS national threat level and to develop corresponding protective measures (Bush, 2002). HSPD-3 encourages voluntary conformity from other levels of government and the private sector. Efforts, such as the Ready Campaign (United States Department of Homeland Security [DHS], 2008) and National Preparedness Month, try to educate the American public about the HSAS and what actions to take when the threat level is elevated.

Numerous problems with HSAS implementation have been identified by stakeholders, Congress, and the media. The most notable recommendation has been to integrate into the HSAS risk communication principles (Government Accountability Office [GAO], 2004, 15), which would presumably facilitate a more effective exchange of information about the risk of terrorism. In the absence of such principles—because it was built without them—the HSAS has been poorly understood, heavily critiqued, and ultimately ineffective in meeting its intended purpose. The consequences have been widespread emotional overreaction by the American public and massive financial impacts to political subdivisions. These consequences have been confirmed through TOPOFF (Top Officials) exercises, Government Accountability Office reports, and summaries from the Congressional Research Service (CRS).

According to the principles of risk communication, terrorism threat information should be consistent, accurate, and clear; provided repeatedly through multiple methods; provided in a timely fashion; specific (nature, timing, location); and provided with guidance on protective measures (GAO, 2004). The threat information specifics are difficult to obtain because they are dependent upon detection of terrorists and their plots through counter-terrorism intelligence. The notion of improving the HSAS through the provision of threat specifics while warning the American public, as HSPD-3 requires, places the HSAS in conflict with prevention efforts.

B. RESEARCH QUESTION

Can terrorism warnings to the American public be improved by utilizing risk communication principles with the HSAS? If not, how should the U.S. Department of Homeland Security handle risk communication with the American public regarding terrorism threats?

C. HYPOTHESIS

This research begins with the assumption that the HSAS is flawed, but it proceeds from the suspicion that the flaws may be unfixable because the need to employ risk communication principles and the challenges that result from such an employment are irreconcilable. Some of the problems with the HSAS may in fact be intensified, rather than overcome, by traditional risk communication principles because of specific public communication issues unique to terrorism. It is anticipated that research will call into question the reasoning behind the desire to warn the public about specific threats of terrorism. Sustaining a system regardless of its ability to effectively achieve its stated purpose with the American public may stem from perceptions of political necessity following September 11. The effects of sustaining the system will be explored, and findings will frame the recommendations for future HSAS policy.

D. LITERATURE REVIEW

The core documents pertaining to the foundation, mission, design, and functions of the HSAS are Homeland Security Presidential Directives 3 (HSPD-3) and 5 (HSPD-5). There are also numerous reports from the GAO, CRS, and other sources that have criticized various aspects, flaws, and consequences of the system. Public Law 110-53, implementing recommendations of the 9/11 Commission Act of 2007 (United States Congress, 2007b) required changes to the HSAS and resulted in the establishment of a bipartisan task force under the Homeland Security Advisory Council. The Homeland Security Advisory System Task Force Report and Recommendations review is a first step toward implementing the requirements of Public Law 110-53.

Criticism of the HSAS has resulted in the analysis of technological tools as possible solutions to better communication of warnings. The CRS Report for Congress: The Emergency Alert System (EAS) and All-Hazard Warnings evaluates the EAS as a possible solution to terrorism threat advisories in the future. Executive Order 13407 (Bush, 2006) requires advancement of the EAS. This executive order tasks the Secretary of DHS with enhancing EAS communications to reach cell phones, personal digital assistants and text pagers within specific geographic areas and specific groups. This was done to ensure that the president can communicate with the American public at all times, including during instances of war, terrorism, natural disaster, or other hazards. Executive order 13407 led to the IPAWS (Integrated Public Alert and Warning System) initiative being coordinated by FEMA, within DHS.

IPAWS implementation has been challenging, and it has been criticized. U.S. congressional hearings have been important in detailing and documenting problems faced by FEMA. In a statement before the U.S. House of Representatives Subcommittee on Economic Development, Public Buildings, and Emergency Management (2008a) the Honorable James L. Oberstar summarized the challenges to IPAWS as resulting from a lack of planning for the future. It was also noted, during a hearing of the U.S. House of Representatives Committee on Transportation and Infrastructure Oversight and Investigations (2008b), that FEMA's challenges with IPAWS are linked to legacy

problems stemming from EAS. A history of different roles between levels of government, the public, and private sectors has led to coordination problems and inconsistent utilization of EAS within and among states. A *Federal Computer Week* article, "FEMA Adopts Open Standards" (Lipowicz, 2008), emphasizes that IPAWS is not a simple technology solution. No single system will work for all jurisdictions, and a meta-systems approach requires partnerships with new stakeholders and those from the EAS era.

What is communicated in a warning is just as important as how it is communicated. Understanding about the necessary substance of a message comes from a long history of risk communication on natural hazards, technological accidents, and missing children. In critiquing the HSAS, the GAO publication "Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System" (2004, 15) recommends that risk communication principles be used with the HSAS to facilitate the effective exchange of information on the risk of terrorism. According to this GAO publication, when these principles are applied to a terrorism threat the information should be: consistent, accurate, and clear; provided repeatedly through multiple methods; provided in a timely fashion; specific about the threat (nature, timing, location); and provided with guidance on protective measures. A Partnership for Public Warning publication, "Protecting America's Communities: An Introduction to Public Alert & Warning" (2004), explains that using risk communication principles increases the likelihood that recipients of the warning will take protective action. This is a challenging process that requires gaining the public's attention through accurate and relevant information that is timely enough for people to react.

The specificity of shared information and timeliness that these principles require is uniquely problematic in the case of terrorism. In the article, "Delivering Clear and Effective Warnings: Applying Lessons from Natural Hazards to Terrorism," Dr. Peter Ward (2002), of the Partnership for Public Warning, notes that risk communication related to terrorism is unique from other hazards because terrorists can interact with warnings. Too much information distributed to the public regarding a terrorism threat can aid terrorists in achieving their goal of successful attack. Without specific information, however, terrorism warnings become questionable as to their effectiveness and can cause

unintended consequences. In an article titled “The Political Psychology of Terrorist Alarms,” Dr. Philip Zimbardo (2003) claims that warnings lacking specificity cause fear. The article roots terrorism in psychology and points out that terrorism is strategic action to incite fear. Vague and false alarms do the work for terrorists, creating heightened and sustained anxiety and confusion within the American public.

These hazard-specific problems call into question the purpose of the HSAS. Dr. Batya Ludman in an Israel News Agency article, “Israel Leads in Making Terror Warnings Effective” (2004), states that terrorism is fear inducing because the threat lacks predictability as to when, where, and how attacks may occur. The efforts of counter-terrorism intelligence are aimed at finding answers to these questions in order to prevent an attack from occurring. HSPD-3 and HSPD-5 are seemingly incongruent with prevention efforts if directed toward the American public.

E. METHOD, OUTPUT, AND GOALS

The research of this thesis is intended to advance the understanding of terrorism-related risk communication with the American public. Existing literature on risk communication is abundant for hazards other than terrorism. The small amount of literature related to terrorism risk communication is either watered down by grouping terrorism with “all-hazards” or limiting it to problem identification with the HSAS. This research will attempt to merge these two areas of literature and build on them, utilizing the tools of policy analysis. Conclusions will be drawn with the understanding that unforeseen future changes in technology, politics, and society will require continued review of this subject matter and related policy. It is anticipated that this research will help those future efforts and decision makers.

F. OVERVIEW OF CHAPTERS

Following the introduction to research on this topic, Chapter II describes the history of terrorism threat advisories in the United States, the HSAS itself, and the related problems that have been identified with this system. Chapter III discusses the fundamentals of public warnings and their relationship to terrorism and the HSAS. It will

provide a broader and more in-depth review of the issues surrounding the communication process. Chapter IV concludes the research with a summary analysis of previous chapters and discusses aspects of American politics relevant to this topic. Chapter V makes final policy recommendations for the United States regarding the HSAS and terrorism risk communication to the public.

II. THE HISTORY OF TERRORISM THREAT ADVISORIES IN THE UNITED STATES

A. THE HOMELAND SECURITY ADVISORY SYSTEM

The Homeland Security Advisory System (HSAS), necessitated by the terrorist attacks of September 11, 2001, was created and established in 2002 by President George W. Bush through Homeland Security Presidential Directive 3 (HSPD-3). The HSAS (Bush, 2002) was the administration's answer to an alarmed public that demanded to know more about government actions to prevent terrorism. The system was established to set a wide-ranging and effective way to disseminate information to all levels of government authority, the private sector, and to the American people regarding the risk of terrorist attacks. It was designed to establish a common language and method for sharing terrorist-threat information and to detail the actions that should be taken in response to those threats.

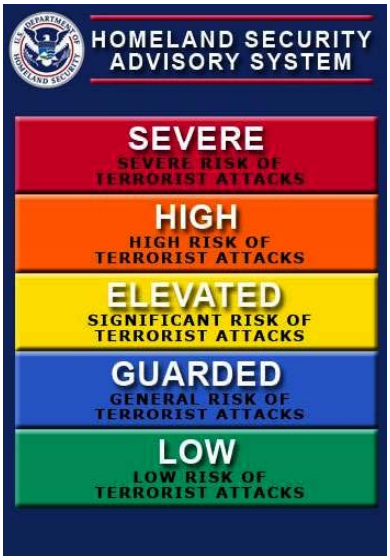

Figure 1. Graphic image of the Homeland Security Advisory System (Source: Department of Homeland Security)

The HSAS (Bush, 2002) directs all nonmilitary federal agencies to ensure that their counter-terrorism operations are consistent with the respective HSAS color-coded threat level and to develop corresponding protective measures. HSPD-3 encourages voluntary conformity from political subdivisions and the private sector. Efforts, such as the Ready Campaign (DHS, 2008) and the September National Preparedness Month, have been attempts to educate the American public about the HSAS and the actions to take when there is an elevated threat level.

HSPD-5, issued in 2003, amended HSPD-3 and gave the responsibility for designating threat levels through the HSAS to the Secretary of the U.S. Department of Homeland Security, which is still the case today. Setting the threat level is done in consultation with the U.S. Attorney General (Bush, 2003), other appropriate federal agency directors, and members of the President's Homeland Security Council. In order to change the threat level, DHS must understand threat information from a variety of sources. DHS receives threat information from multiple sources (GAO, 2004), including but not limited to the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Counter-Terrorist Center (NCTC). Threat levels are intended to be applied to the entire nation (Bush, 2002), a specific geographic area, or to certain industrial sectors. Communicating a change in the threat level has been accomplished through electronic notification (Reese, 2008) from the National Law Enforcement Telecommunications System (NLETS). DHS also makes notification to elected and appointed officials and other stakeholders through conference calls, e-mail, or electronic communications before the public is notified through a press conference and resulting media coverage.

According to the DHS (2008), since its establishment in March of 2002, the HSAS has remained at code yellow—or elevated alert—except for the eight periods in which it was raised to code orange, or high alert. There has only been one instance, in August 2006, when the HSAS was raised to code red, or severe alert (DHS, 2008), and that instance was specific to flights from the United Kingdom to the United States.

B. EXPANDED UNDERSTANDING OF PROBLEMS WITH THE HSAS

Understanding the challenges that have come from the HSAS requires analysis of its real-world application absent a terrorist attack and its simulated application after an exercise-scenario-based attack. The latter has generated much discussion and many worthwhile recommendations regarding the HSAS. Exercising a national system with stakeholders at all levels of government is no small effort and has required Congressional action. Reacting to global terrorism, such as the 1995 Aum Shinrikyo subway Sarin gas incident, the U.S. Congress determined (Department of State, 2002) that top U.S. government officials should be better prepared to address terrorism involving the use of weapons of mass destruction (WMD). In 1998, Congress mandated that the Department of State and the Department of Justice conduct a series of full-scale multi-jurisdictional exercises involving response to a WMD terrorist attack. The result was the TOPOFF (Top Officials) exercise. Beginning with TOPOFF 2000, there have been four TOPOFF exercises.

The TOPOFF exercise series has been the only way to test the process for raising the HSAS, communicating threat information, and understanding related impacts to those with law enforcement, protective measures, or countermeasure responsibilities. TOPOFF 2 was the first test of the system; held from May 12 to 16, 2003, it was the largest and most extensive terrorism response exercise in U.S. history (DHS, 2003). It tested the HSAS with the first-ever elevation to code red, or severe alert. Exercising that elevation gave federal agencies their first opportunity to test their response actions and allowed participants and evaluators to examine the implications. The same was found for those local jurisdictions that raised their own threat levels to red.

Ultimately, TOPOFF 2 found that modification to HSAS implementation was required (DHS, 2003). According to the 2003 TOPOFF 2 After Action Summary Report, there was a lack of awareness of local threat advisory systems, inconsistent or nonexistent formal notification protocols for elevation in the HSAS, and lack of a common

language for communicating elevations. There was also uncertainty among federal agencies about the necessary protective actions in response to code red, and there was confusion about other agencies' actions.

The resulting recommendation was to develop and coordinate responses to HSAS elevations among federal agencies and with political subdivisions (DHS, 2003). It was suggested by participants that responses be tiered in correlation to the HSAS threat levels and be specific to the type of threat. Four years later similar challenges were observed during TOPOFF 4 (DHS, 2007). The TOPOFF 4 After Action Quick Look Report observed that the HSAS threat levels lacked clarity of purpose, definition, and consequences. The resulting recommendation was to review and revise HSAS policy, synchronize HSAS with other alerts, and clarify the protective actions necessary for each threat level and sector (DHS, 2007).

Exercises have not been the only source of criticism of the HSAS. Responding to government agencies' questions about the quality of threat information provided by DHS, and the costs incurred from responses to changes in the threat level, both the Congressional Research Service and the General Accounting Office have looked closely at the HSAS and offered recommendations to Congress for improvement. According to the CRS (2008), there are numerous issues associated with HSAS and how it affects political subdivisions, the public, and the private sector. These include vagueness of warnings; lack of specific protective measures; inadequate dissemination of warnings; poor coordination of HSAS with other federal warning systems;[1] and the cost of threat-level changes. On the other hand, GAO (2004) examined the decision-making process for changing the threat level; the application of risk-communication principles to information sharing within government; protective measures used during code orange, or high alert periods; and the costs associated with those periods. The Government Accountability Office (2004, 15) recommended that risk-communication principles that are employed with other hazards, such as bad weather, be used with the HSAS to facilitate the effective

[1] Other federal warning systems include Department of Defense (DoD) use of the Force Protection Condition (FPCON) and U.S. Coast Guard use of the Maritime Security Threat System (MARSEC).

exchange of information on the risk of terrorism. This is the single most important finding and recommendation. Tables 1 and 2 summarize the key points of criticism and recommendations, respectively.

Table 1. Summary of Criticisms of the Homeland Security Advisory System (HSAS) (Source: Congressional Research Service, General Accounting Office).

1	There is a lack of awareness of local advisories in relation to the HSAS. This suggests a lack of buy-in from stakeholders and limits the HSAS scope to the federal government.
2	There are insufficient notification protocols for elevations in the HSAS threat levels. There is a related lack of common language to communicate elevations.
3	There is uncertainty regarding necessary protective measures required during elevations.
4	The HSAS threat levels lack clarity of purpose, definition, and consequences.
5	There is poor coordination of HSAS with other federal warning systems.
6	There are high costs associated with elevation in HSAS threat levels.
7	There is a lack of risk-communication principles and documented communication protocol.

Table 2. Summary of Recommended Changes to the Homeland Security Advisory System (HSAS) (Source: Congressional Research Service, General Accounting Office).

1	Develop coordinated responses to elevations by using a tiered operational response framework.
2	Synchronize the HSAS with other systems or consolidate all federal warning systems.
3	Clarify necessary protective actions by level and sector.
4	Use specificity in elevations of the HSAS threat advisories.
5	Limit the scope of the HSAS to federal agencies.
6	Have DHS develop protective action guidance for political subdivisions, the private sector, and the public.
7	Use technology to better disseminate HSAS threat advisories.
8	Allow existing homeland security grants to states and localities to address costs associated with HSAS elevations or establish new and specific HSAS grants for this purpose.
9	Document HSAS communication protocols.
10	Incorporate risk-communication principles into the HSAS.

Criticism of the HSAS, and recommendations for change, have driven attempts at legislated improvement. The 108th [2] and the 109th [3] Congresses have previously proposed several bills to modify or replace the HSAS, but none was ever successfully enacted. It was not until the 110th Congress and the Implementing Recommendations of the 9/11 Commission Act of 2007 (United States Congress, 2007b) that change to the HSAS was legislated. That law requires the DHS Secretary to administer the HSAS in a manner that warns government of domestic terrorism threats, and the American public as appropriate. Specifically, it requires the Secretary to establish criteria for the issuance and revocation of advisories; develop a methodology for issuance and revocation; provide specific information and advice on protective measures; limit the scope of advisories to specific regions, localities, or sectors; and refrain from using color designations exclusively to specify threat levels. These legislated changes were not novel and are consistent with previous recommendations for change. Still, apart from the few minor adjustments in sector specific application by DHS in 2006, the HSAS has been relatively unchanged since the enactment of Public Law 110-53. The HSAS threat levels have not been adjusted, elevated, or lowered since that time.

On July 14, 2009, President Barack Obama's newly appointed DHS Secretary, Janet Napolitano, ordered a sixty-day review of the HSAS and its effectiveness in warning Americans of terror threats and providing them with information on related protective measures (McCarter, 2009). The review was under the Homeland Security Advisory Council's bipartisan task force, chaired by Fran Townsend and Judge William Webster. Membership included elected officials, law enforcement, and private-sector security experts. The task force review is a first step in implementing the requirements of Public Law 110-53. During the review, the task force accepted input from the public and subject matter experts such as former DHS Secretary Tom Ridge. In September 2009, the Homeland Security Advisory System Task Force Report and Recommendations was published.

[2] From the 108th Congress: House Bill 3266; Senate bill 118; and House Bill 2537.

[3] From the 109th Congress: House Bill 2101; Senate Bill 1753; and House Bill 5001.

The report was summarized into six main points. These points affirmed the need for the HSAS, noting its continued relevance to homeland security efforts. The report stated the need for the HSAS to remain dedicated to terrorism and not to become aligned with other national warning systems. It acknowledged that the HSAS has an audience in government, nongovernmental organizations, and the American public. It confirmed that communication with the public has been poor, causing a lack of confidence in the system that must be fixed. It also noted the need for the HSAS to be reset to a new default baseline guarded status. The report explained the need for specific warnings and protective measures applicable to threatened localities, first responders, and private-sector companies. Lastly, it claimed that the Secretary needs dedicated HSAS resources, staff, protocols, and procedures.

The report's recommendations focused on the six summarized points and were divided into five categories: threshold conclusions; recommendations for the whole system; recommendations specific to the general public; recommendations specific to institutional players; and infrastructure for the future. The twenty recommendations are summarized in Table 3. Any adopted recommendations or other changes come from the President.

Table 3. HSAS Task Force Report Recommendations for the Secretary (Source: Homeland Security Advisory System Task Force Report and Recommendations).

Threshold Conclusions	
1	Remain exclusively focused on terrorism
2	Four identified vulnerabilities with the current system
Recommendations for the Whole System	
3	Provide the fullest degree of information possible, declassify, and disclose
4	Secretary's communication should be ongoing, regular, and coordinated with states and localities
5	Develop a common vocabulary for threat levels across the federal government
6	Offer transparency on the process used to make alert decisions
7	Set a new guarded baseline for the system
8	Target threat alerts to specific locations and sectors at risk
9	Regularly reassess the system and lower threat levels when threat information permits
10	Secretary should debrief threats and what has happened to them
Recommendations Specific to the General Public	
11	Retain targeted risk communication with the public
12	Reduce the system to three levels
13	Do not substitute threat levels for full disclosure of information
14	Stay current with new media and ways to communicate
Recommendations Specific to Institutional Players	
15	Target threat alerts to specific locations and sectors at risk and revisit decision merits every 15 days
16	Convey the same message meaning for both the public and institutional players
17	Develop a plan and protocol for reaching institutional players
18	Secretary should review DHS capability to communicate sophisticated and technical information
19	Utilize fusion centers and JTTFs as point of contact for state information
Infrastructure for the Future	
20	Strengthen the system with dedicated resources, staff, protocols, and procedures

III. CONTEXTUAL UNDERSTANDING OF PUBLIC WARNINGS

A. BACKGROUND AND MECHANISM OF PUBLIC WARNINGS

Warning is a seemingly simple term to understand. When a warning is given, it is an attempt to notify a person or group about a threat in advance of harm. A warning should include an instruction to either do something, or not, which will ultimately help protect the recipient or help counter the threat. A historical example of this in America is the 1775 Paul Revere ride from Boston to Lexington to warn people of British Army troop movements. In this example, Paul Revere was a credible messenger delivering a clear and specific warning that motivated people to action and resulted in the defeat of the British at Concord (Zimbardo, 2003). Contextually, this example of warning is straightforward. However, substituting terrorists for the British and the American public for the militia, it becomes clear that warning about the threat of terrorism is not similar to the Paul Revere warning. Granted, both are related to preserving life from violent attack, but the threat and target of attack are different, which has a significant impact on the warning message. Terrorism is specific to clandestine threats, which makes it hard to achieve clear and specific message content. Terrorism also targets more than military forces, which makes the effectiveness of the message more difficult because of the variance and complexity of the audience. It is the intentional predation on noncombatant civilians using the element of surprise that sets terrorism apart from other threats. These elements challenge the notion of effective warning and warrant contemplation in relation to message content.

The warning act itself is clear-cut. It is intrinsic human behavior meant for survival. One can see it in its most basic form with alarm calls (Weiss, 2005) and SOS screams that primates use as a pure life-saving strategy against predators (Zuberbuhler, 2007). Humans have retained this same innate anti-predation behavior throughout evolution (Treves & Palmqvist, 2007). This built-in warning behavior was even present on September 11, 2001. The onboard activity of United Airlines Flight 93 after the plane was hijacked on the morning of 9/11 shows that passengers used GTE air phones and

cellular phones to contact authorities, relatives, and friends (National Commission on Terrorist Attacks upon the United States [National Commission], 2004). Through these calls, the passengers became aware of the other planes that had been flown into the World Trade Center. Through social networking, passengers were warned of the terrorism threat. The instinctual "alarm calls" gave information that resulted in action from a few of the passengers against the hijacking terrorists. This ultimately led to Flight 93 not reaching its intended target—the White House or U.S. Capitol—and instead crash landing in a Shanksville, Pennsylvania, field, killing all on board, including the terrorists (National Commission, 2004). The Flight 93 example of warning illustrates our human conditioning to tell others about danger and to be receptive to such warnings. Unfortunately, Flight 93 warnings did not result in survival for those who received it. The warnings came too late.

What HSPD-3 directs the United States to provide to citizens is information akin to the Flight 93 warnings, albeit earlier and with more confidence. This is significantly more complex than warning from person to person. National-level warnings are a more complicated social process than interpersonal communication (Smelser, 2007). The former messages must be received and understood by a diverse society in order to influence behavior. With this in mind, it is easy to understand why risk-communication principles have been recommended for warnings from the HSAS. Risk communication is well researched and studied in the context of natural and technological hazards. Testing and applying risk communication over time has led to an understanding that empowering people to make informed safety decisions is easier when necessary and specific information is provided (Partnership for Public Warning, 2004). In essence, the application of these principles to terrorism is an attempt to provide the public with specifics on the threat to improve the likelihood that protective action will be taken. When this has not been the case with HSAS warnings, there is evidence of significant consequences. The most notable of these is widespread emotional overreactions and massive financial impacts. A nationwide survey (United States Conference of Mayors, 2003) showed that cities spent about $70 million per week in orange-alert-related direct

expenses.[4] These unbudgeted expenditures could not be sustained (Reese, 2008) and did not provide the security that was intended. Vague warnings have also been shown to incite fear in the public (Zimbardo, 2003). By creating heightened and sustained anxiety and confusion among the American public, unspecific warnings spread fear the way terrorists do (Zimbardo, 2003).

Criticism supported with factual data did bring about change in HSAS application. The best example of the attempt to improve message effectiveness is the August 2006 HSAS elevation to code orange for commercial aviation coming to the United States and to code red for flights originating from the United Kingdom (United States Department of Homeland Security [USDHS], 2008b). The elevation was the direct result of a disrupted terrorist plot to bomb aircraft destined for the United States from the United Kingdom using liquid explosives. This identification of threat, tactic, and vulnerability was used to provide a specific threat advisory and has resulted in the 3-1-1 liquid carry on policy (3 oz. or less, 1 quart-size bag, 1 bag per passenger) enforced by the Transportation Security Administration (Transportation Security Administration [TSA], 2009). Specificity enabled preventive measures and protective actions to be tailored to the threat and vulnerability. This action was taken without unnecessarily impacting other stakeholders or sectors. On the surface, these changes appear to be a successful application of the recommended risk-communication principles. Clearly, the HSAS can be implemented with the provision of threat specifics. However, the specifics must be provided in a timely manner in order for those who are threatened to take protective action. The August 2006 advisory was reactionary and did not allow for this. It came after the threat had passed, when the plot was already disrupted and the adversaries had been interdicted. It did not demonstrate that it could have provided threat specifics without that information aiding the terrorists behind the threat. If the warning did provide these details before detection and disruption, it would have been widely distributed through the media to a broad public audience that included the terrorists. Advising adversaries that there were going to be enhanced security measures at airports concerning

[4] According to the survey, Phoenix spent $154,000 on a weekly basis, Los Angeles spent $2.5 million each week, and New York City spent $5 million each week.

liquids would have afforded them an opportunity to modify attack planning, better evade law enforcement, and increase the potential for a successful attack.[5]

Unfortunately, this example represents the last change in the HSAS threat level before the Homeland Security Advisory System Task Force Report and Recommendations was published.[6] It has sat unchanged for over three years. Being stagnant shows not only that the 2006 change in HSAS application was not a solution, but also, that there remain inherent problems with messages regarding terrorism. It is not intended to be a general health awareness campaign like those used by the government to warn of the dangers associated with drinking and driving, unprotected sex, or the use of tobacco products. This type of terrorism awareness is already available, such as from the previously mentioned Ready Campaign and National Preparedness Month (USDHS, 2008c). HSAS warning messages must include information about terrorists and their plots in order to increase the chance that those messages will aid in survival. This is not straightforward like warning instinctually or about an approaching hurricane. The warning message is problematic for counterterrorism prevention efforts, if it discloses intelligence-based details to the public. It is counterproductive and dangerous to communicate risk in a manner that enables our adversaries or serves their objectives.

B. MESSAGE DELIVERY: TECHNOLOGICAL DEPENDENCY

The August 2006 warning is also useful in understanding that, due to the delay in issuance of the warning, the American public would have been unaware that they were potential victims of an attack had the terrorist plot not been disrupted. Prevention of the terror attack fortunately also prevented this warning problem. This will not always be the case. Future prevention is not guaranteed and may unfortunately bring other attacks like that of 9/11. If it is U.S. policy to reach vulnerable people with a warning message when

[5] None of the recommendations proposed in the September 2009 Homeland Security Advisory System Task Force Report place counterterrorism intelligence for prevention above risk communication with the public. Not distinguishing between these audiences, while also recommending increased transparency in issuance decision making and increased specificity in warning content does not alleviate the problem of informing and aiding terrorists.

[6] The attempt to bomb and destroy Northwest Airlines flight #253 on Christmas Day 2009 on its way to Detroit from Amsterdam did not result in any change to the HSAS.

these times come, the way and means in which this will be achieved must be determined. Clearly, the message must reach the right people with accurate and relevant information regardless of time, location, or special needs that the recipient might have (Covello, McCallum, & Pavlova, 2004). In the 2006 example, there was no specific identified threatened population and no way of exclusively warning them if they had been. In order to be effective, future terror warnings must address whom to warn and how to warn them, without disclosing intelligence at the expense of law enforcement. This means sharing detailed threat information in a timely manner using fail-proof communication with only those who are threatened. This would fit the targeted risk communication with the public recommended in the Homeland Security Advisory System Task Force Report and Recommendations. The big question is how this is to be done.[7] You cannot warn someone if you cannot communicate with him.

Reaching those who are threatened depends on available technology. In the past, the medium was ultimately the HSAS messenger. There was no standardized or personal way for government to communicate warnings. Various competing media outlets would broadcast varied messages based upon the facts they received from DHS or other officials. Technology use was relegated to those who chose to listen or view what the media had to say on the matter. This has not been the case for other government efforts to communicate with the public about other hazards. The Emergency Alert System (EAS) has been the historical standard for government risk communication. The EAS is a federally managed warning system (L. K. Moore, 2009) administered by the Federal Emergency Management Agency (FEMA) and the Federal Communications Commission (FCC). It is administered as an all-hazard warning capability in cooperation with the National Weather Service (NWS) and is broadcast on National Oceanic and Atmospheric Administration (NOAA) weather radios (L. K. Moore, 2009). The FCC (2008) requires that all radio and television stations have EAS capability. It is generally understood that EAS messages interrupt programming on radio and television to provide short and specific information regarding an emergency situation. When EAS began to be used with

[7] According to the Partnership for Public Warning (2004), details such as this should be conveyed to the public for management of expectations. Public education helps clarify how people will be warned and what the warnings mean.

the AMBER Alert System (National Center for Missing & Exploited Children [NCMEC], 2008), it also allowed for specific information to be provided about perpetrators and vehicles, which can be broadcast on electronic highway billboards. This capability has been incorporated into discussions about how to fix the HSAS.

In June 2006, President George W. Bush issued Executive Order 13407, which requires expansion of the EAS. This executive order tasks the secretary of DHS with enhancing EAS communications to reach cell phones, personal digital assistants, and text pagers within specific geographic areas and specific groups. This was done to ensure that the president can communicate with the American public at all times, including during instances of war, terrorism, natural disaster, or other hazards. This has led to the IPAWS (Integrated Public Alert and Warning System) initiative being coordinated by FEMA. According to FEMA (2008), IPAWS is the next generation in public warning. FEMA's IPAWS Program Management Office was established to take the vision that was set out in President Bush's 2006 executive order and oversee the evolution from EAS technology to more personal and modern forms. Warnings, once limited to media broadcasts through television and radio, are intended to be communicated in a personalized manner to all Americans in the near future, including languages other than English and to those with hearing and vision disabilities. Table 4 is a conceptual comparison between HSAS and IPAWS based upon three key related risk communication principles.

As FEMA puts it, IPAWS will improve terrorism threat advisories by communicating with as many people as possible through as many communication devices as possible. To accomplish this, FEMA intends to pull several capabilities together into a metasystem. Current progress towards this end is found in FEMA pilot programs

operating in fourteen states throughout America.[8] These pilots are a window to the future of the IPAWS metasystem. The Washington Post reports (Hsu, 2006) that these pilot programs were initially supported by $25 million in appropriated funds from Congress. Initial sustainment funding was provided for IPAWS in the DHS 2009 appropriations. There is no sign that this will cease in future fiscal years. Legislature has shown a continued interest through requirement of a conversion plan from DHS and related reporting.

Table 4. Comparison of HSAS and IPAWS Communication Technologies Using Risk Communication Principles (Source: Department of Homeland Security, FEMA).

Risk Communication Principles – Terrorism Hazard	Homeland Security Advisory System (HSAS)	Integrated Public Alert & Warning System (IPAWS)
1) Consistent, Accurate, and Clear Messaging	System, intended for federal government application, lacked policy for communicating risk with the American public.	Intended to communicate risk with the American public via personal communication technology devices.
2) Repeated Messages through Multiple Methods	Communication with the public through the media.	Communication capabilities of EAS are greater than general press releases. IPAWS potential to greatly expand capabilities via cell phones, pagers, PDAs, email.
3) Timeliness	Limited capability due to reliance on media for message dissemination.	Probability of reaching an intended audience increases with enhanced capability to reach the American public via personal communication technology devices.

Other notable events surrounding IPAWS originate from the WARN Act (Warning, Alert and Response Network Act, P.L. 109-347) and the FCC. According to

[8] According to FEMA, some notable pilot projects include Digital EAS (DEAS), a digital technology and international warning standards upgrade to overcome the challenges of digital television. The DEAS initiative is also piloting DEAS in state and territory emergency operation centers to provide alert capability to local officials. The Geo-Targeted Alerting System (GTAS) is a joint project with NOAA through which new technologies are being tested to give emergency managers the ability to predict hazard areas, collaborate, and deliver alerts and protective measure guidance to specific geographical areas. The Web Alert Relay Network (WARN) provides emergency operation centers with web-based collaboration tools and alert capabilities. The alert capabilities allow for opt-in participants to receive messages on their cell phones and pagers. The Emergency Telephone Notification (ETN) provides automated telephone calling to specific geographical areas. Enhanced ETN adds the capability for translation of English into multiple other languages. The Deaf and Hard of Hearing Notification System (DHNS) is emergency communication to the hearing impaired through American Sign Language videos, the Internet, and other personal communication devices.

the U.S. House of Representatives (2008) summary on the IPAWS subject, the WARN Act required the FCC to establish the Commercial Mobile Service Alert Advisory Committee (CMSAAC). The CMSAAC exists to give the FCC recommendations on matters relating to the transmission of emergency alerts by commercial mobile-service providers. The result of CMSAAC efforts and FCC adoption of recommendations is the nationwide Commercial Mobile Alert System (CMAS). The CMAS will transmit emergency alerts to cellular subscribers through commercial mobile-service providers who receive the alert from FEMA, the federal agency aggregator. FEMA has also adopted FCC guidance to use open standard technology, CAP (Common Alerting Protocol), for message dissemination. CAP is a nonproprietary digital message format (Czarnecki, 2008). CAP is capable of sending more than EAS messaging, including video, multiple languages, graphics, and resources for those with communication disabilities.[9] The open system affords an opportunity to bring many private-sector companies into partnership such as cable, telecommunication, software, device manufacturers, media outlets, and IP-based systems. Assurance of interoperability is being addressed through coordination with the National Institute of Standards & Technology.

Not unexpectedly, the activity surrounding the implementation of IPAWS has generated critics and disbelievers. In a statement before the U.S. House of Representatives, Subcommittee on Economic Development, Public Buildings, and Emergency Management (2008a) Congressman Oberstar summarized the challenges to IPAWS as having been born of a lack of planning for the future. There is no clear and agreed-upon vision for what the future system-of-systems will look like. To date, FEMA has invested too much in vendors and contractors and not enough on involving the necessary partners and stakeholders (Lipowicz, 2008). The potential effects of this are great. The IPAWS solution is not one of technology alone as there is no single technology or system that works for all local jurisdictions. To be a true system-of-systems, partnerships must be cultivated and maintained. This applies to the future as

[9] Currently CAP is being used in the DEAS initiative and is interoperable with tools capable of receiving CAP 1.1 messages and sending alerts via satellite radio, cell phones, pagers, computers, and electronic signs (Stine, 2008).

well as to the past. A significant number of partners from the EAS era need to be brought along into IPAWS, partners such as broadcasters, who continue to be capable of reaching many people in a short period of time (Stine, 2008). FEMA's rollout of IPAWS is also challenged (U.S. House, 2008) because in the past the organization has had issues with effective alert dissemination and EAS. A history of different roles between levels of government, the public, and private sectors has led to coordination problems and varying utilization of EAS within states. Next generation EAS, IPAWS, will be contingent upon mending this problem and garnering buy-in from states and localities (Stine, 2008).[10] This is not easily accomplished; however, as it is not yet clear whether FEMA is going to scale IPAWS to localized emergencies (Lipowicz, 2008). The lack of buy-in and progress from FEMA has led some states and localities to proceed with alert-system infrastructure that is not compatible with CAP (Sternstein, 2009). If FEMA does scale IPAWS to localized emergencies, there will be greater potential for local infrastructure to be built with CAP compatibility. It is unclear whether the existing incompatible infrastructure challenge can be overcome. There has been mention that state organization around this issue, such as establishment of State Emergency Communications Committees (SECC), may be capable of building new distribution networks for CAP alerts (Lipowicz, 2008). This, however, has not moved beyond conceptual conversation. Any effort to address incompatible infrastructure would require significant funding that has not yet been estimated. There are also other financial implications associated with a localized IPAWS, such as the considerable training needed to originate effective CAP messages. In 2007, GAO found that EAS was mired in dependability and effectiveness issues because many EAS participants nationwide lacked the training and technical skills necessary to issue alerts.

[10] Challenges and shortcomings may be addressed through future legislation. From the 111th Congress, H.R. 2591: The Integrated Public Alert and Warning System Modernization Act of 2009 proposes criteria for performance and implementation based upon best practices from the emergency and response community (L. K. Moore, 2009). It would authorize $37 million initially and subsequent fiscal year funding to support pilot programs. It would establish the IPAWS Advisory Committee, which would oversee the IPAWS design and implementation. Specifically, the committee would ensure that IPAWS demonstrated system requirements included in the bill. IPAWS is to incorporate multiple technologies, communicate directly with the public, provide alerts widely, and be redundant. IPAWS is also required to promote public-private partnerships for enhanced community preparedness and response. The bill does not, however, require IPAWS to coordinate with the similar work and efforts being undertaken by states and localities.

Ultimately, the reality that IPAWS will meet the vision set by Executive Order 13407 is science fiction at present, and progress is mired in significant challenges. This unfortunate reality is disruptive to the notion of providing timely information to those who are imminently threatened by an unavoidable terrorist attack. IPAWS does not currently allow for the information necessary to save lives to reach people in a personal manner. Even if those with responsibility for detecting terrorists and their plots had information to share with specific threatened populations, they are unable to do so. Changing this and improving efficiency is unlikely as long as the IPAWS initiative is a system-of-systems approach by FEMA that is not effectively coordinated with necessary stakeholders.

C. THE MESSENGER RECEIVER RELATIONSHIP: POWER OF PERCEPTION

> As usual, what we were doing was fodder for criticism, and for satire.
>
> — Tom Ridge

The messenger of a warning is an important determinant of its effectiveness, and the wrong approach can cause even the best message to be ineffective. Success is measured by the actions taken by the public in response to a warning, and this hinges on established credibility and trust of the messenger (Parker, 2005). Being understood as a credible and trustworthy messenger by the receiver is important to message recognition (Pinker, 2007). Trust can be defined as the mental intention to be vulnerable and accept information based upon positive expectations of intentions and behavior of the messenger (Banerjee, Bowie, & Pavone, 2006). Establishing this is necessary for someone to receive and act on shared information (Banerjee, Bowie, & Pavone, 2006). It can take time to develop and is dependent upon positive past experiences and positive perceptions (Banerjee, Bowie, & Pavone, 2006). This is central to understanding why some individuals and organizations are able to share information with positive results. It is believed that how one perceives the messenger is pivotal to effectiveness and determines what action will or will not be taken (Association of State and Territorial Health Officials, 2002). There are at least twenty perceptual factors that have been shown to

influence people's willingness to accept information and assess risk (Jones-Hard, 2004). All of these have relevance to how people perceive the HSAS and terror warnings.[11] To accept this type of information, people want to know and understand that the messenger has these traits. This can help explain why it is still very challenging to incite the American public to protect itself and why some people do not heed hazard warnings. Perceptions can even negate reception of information about the most significant risks (Covello, 1998). Information about terrorism, which can rate high with the public, is still challenged by the complexity of people's perceptions of the messenger (Jones-Hard, 2004).

Messengers must also contend with the nature of terrorism and how it is personally experienced by those being communicated with. The emotional state of the recipient helps determine whether or not he will receive, accept, and act on the message being sent. In the case of terrorism, it is fear that is of most concern for messengers. It has been shown that people are less likely to be receptive to information when it is provided during a crisis (Covello, 1998). The emotional involvement of the message recipient and his feeling of being personally threatened can generate mental noise, an inability to comprehend, which can inhibit one's ability to engage in communication about personal safety (Covello, 1998). Research has shown that up to eighty percent of efficiency and effectiveness in processing information is lost in these situations (Covello, 1998).[12] The high emotional significance of terrorism can also work against trust formation. Those who are anxious, fearful, or upset are prone to distrust because they have a harder time hearing, understanding, and remembering (Covello, 1998).

While fear has been claimed to be an emotional motivator[13] with other hazards, capable of overcoming perception and reception difficulties, this is not the case with

---

[11] The message influence model, which states that the message sent is what counts, is flawed. Listeners create meaning to messages based upon perception factors. What results will most likely not be identical to the messenger's intent. The receiver and the message he receives is what counts (Corman, Goodall, & Trethewey, 2007).

[12] This loss is even greater when information is provided electronically (Covello, 1998).

[13] It has been suggested that fear-inducing communication can motivate people to take fear-reducing action (Boer & Seydel, 1996). If given advice on ways to reduce the threat and remain safe, people are believed to be more likely to comply based upon their experienced fear.

terrorism (Boer & Seydel, 1996). Terrorists take advantage of and benefit from public fear, regardless of whether it is created by an attack or the threat of one. It is common for people to be afraid of what they do not understand or are unfamiliar with (Winters, 2002).[14] Even that which is nonthreatening can cause fear if it is unknown. This is why people tend to fear terrorism more than other hazards (Ripley, 2008). It also explains why the relationship between the nature of the threat and characteristics of the hazard are problematic for warning messengers. Warning someone of the likelihood of his death at the hands of terrorists can create the same fear and associated adverse reactions (Ripley, 2008). Messengers who rely on press and news outlets to communicate must also be wary. The American media,[15] while chasing viewership and ratings, has become known to researchers as a partner of terrorists by repeatedly spreading negative messages and images to the public since 9/11 (Breckenridge & Zimbardo, 2007). Negativity bias drives coverage of negative events because our attention and memory is programmed in our brains to prioritize negative and high-arousal stimuli (Breckenridge & Zimbardo, 2007). The effects of this are not easily overcome or forgotten. Emotion memory, heuristics,[16] and its implications on behavior are all working against the messenger's efforts. The result can be an unmotivated and fearful public, prone to denial of threat information and avoidance of the messaging (Covello, McCallum, & Pavlova, 2004). Messenger efforts must understand that hearing, comprehending, and remembering are better achieved through efforts to reduce fear and enhance safety rather than inducing it (Partnership for Public Warning, 2004).

---

[14] Winters's example of the problem with fearing the unknown is the murder of Balbir Singh Sodhi on September 15, 2001, in Mesa, Arizona. Mr. Sodhi was murdered because of the turban he wore and the color of his skin, despite not being Arab, Muslim, or a terrorist.

[15] The media should be seen as being made up of community representatives no different from others that new U.S. policy and strategy should be geared towards. The same holds true for the politicians necessary for policy change. The audience that government appeals to for future education on the nature of terrorism should be all inclusive.

[16] Perceptions, personal beliefs, are shaped by past emotion-laden experiences (Ripley, 2008). Emotions such as fear are used as information by the brain in order to determine what course of action to take (Breckenridge, 2010). This is done without intentional thought (Breckenridge, 2010). The brain calls upon emotional memory shortcuts to influence intuitive subconscious assessments of risk and decision making (Kahneman, 1979). It is only after the fact that we are able to justify for ourselves why we acted the way we did (Breckenridge, 2010).

Regrettably, the circumstances are stacked against government. Thus, much of the research into understanding America's experience with public risk communication difficulties has focused on mistrust of government. Americans for the most part consider government to be a less credible source of information during a crisis when there is a lack of trust. A 2004 Gallup Poll (Parker, 2005) showed that 31 percent of Americans had little or no trust in their local government, 32 percent said the same of state government, and 41 percent said the same of the federal government. This followed previous 2003 Gallup Poll findings (D. Moore, 2003), which showed that most Americans were not taking steps to prepare for terrorism despite HSAS alerts.[17] Only four out of ten respondents in that poll believed that HSAS alerts were serious and applied to them. This lack of trust in government stems from negative past experiences and public perceptions of DHS and the HSAS. This can be attributed to leadership, their qualities, and individual behavior (Dirks, 2006). Leaders face great scrutiny in the decisions they make and their communications about terrorism. They are judged more severely with matters of safety. The public's concerns about life and death have great bearing on homeland security leaders' ability to communicate terrorism risk through the HSAS. Greater scrutiny of their actions increases the likelihood that expectations will not be met. Because of this, it

[17] Some reasons offered included the government being unwilling to recognize problems, share information, and allow public participation. The public also perceives the government as being insensitive to concerns and deficient in carrying out safety responsibilities (Moore, 2003).

is harder in this arena to obtain trust (Kramer, 2006)[18] and even harder to mend broken trust relationships (Banerjee, Bowie, & Pavone, 2006),[19] which may exist from past application of the HSAS.

Uncongenial approaches that are distant from the public and layered with government formality only exacerbate the problem that homeland security leaders face in public communication. As seen with the history of the HSAS, top-down messaging from the federal government to individuals regarding terrorism is not the most effective way to communicate because the necessary traits for trust determination are hard to assess when there is little or no personal familiarity with the messenger (Banerjee, Bowie, & Pavone, 2006). It is believed that trust is better established from local government approaches to addressing the public (Partnership for Public Warning, 2004). Not only are local jurisdictions the first to experience an impact and ultimately left to recover, they are also represented by people who share in the community's experience. This aids positive perception. The traits that determine trust are found more readily when the messenger is close to home, like a local government official. Terrorist attacks, despite being a unique man-made hazard with national implications, are no different in the sense that they begin and end locally. It is logical, then, to assume that the best messenger of a terrorist threat warning would also be a local government leader with responsibility for the threatened jurisdiction.

[18] As an example, physician and patient relationships demonstrate the significance of scrutiny and life preservation on trustworthiness. The dynamic between the physician messenger and patient receiver is significant for trusting the communicated message and taking appropriate action directly related to health and well-being. Thus, as patient scrutiny of behavior increases so does the likelihood that negative judgments will be made about the trustworthiness of the physician. It is less likely in this setting that appropriate action will be taken for one's own health. Further, this physician-patient relationship has been shown to be significantly impacted by managed care settings (Kramer, 2006). The trust in communication that results in action is significantly diminished in team medical settings with institutional practices and policy. The trust that can be envisioned as resulting from a home visiting family physician is lost in institutionalized settings. Perceptions that form trust are not only challenged due to the scrutiny placed on behavior related to health and safety, they are also limited when a person is faced with more people, bureaucracy, and complex impersonal processes.

[19] If trust is damaged it is not easily recovered and requires different approaches than gaining it to begin with. The mistrusting must reestablish expectations and overcome negative perceptions associated with the event that damaged the trust. The trust attempting to be reacquired can be significantly greater than that which was initially developed (Banerjee, Bowie, & Pavone, 2006).

Taking into account the content requirements for an effective message, the notion of local terror warning implies that there is an intelligence capability to support the messenger. If public warning were to occur locally, state and local fusion centers and capabilities would have to be considered as a way of making that possible. Fusion centers in concept are intended to counter top-down approaches to prevention by fusing together different disciplines, levels of government, and in certain instances the FBI's Joint Terrorism Task Force (JTTF). It is claimed that information can be collected and analyzed locally, shared at the national level for big picture analysis, and returned to the local level to continue the intelligence cycle and aid in prevention (Osborne, 2009). Incorporating local law enforcement into the intelligence community could be advantageous because it would put boots on the ground in communities across the nation (Bettenhausen, 2008). This capability is unique to local government and is claimed to enable local and state law enforcement to better detect future terror plots (Squires, 2009). Colocation within fusion centers is intended to aid in successfully overcoming the complexity inherent in this type of government collaboration and in achieving the desired homogeneous effort towards prevention.

Still, these advantageous qualities are not aimed at risk communication. The fusion center philosophy remains one of prevention, to uniquely investigate, collect, and analyze intelligence to enhance counterterrorism efforts (Nenneman, 2008). Consideration of adding the duty of publicly warning is significant and unprecedented. Doing so puts nonprevention-based objectives in competition with resources dedicated to counterterrorism's greatest priority. Still, warning the public over private networks and systems has been encouraged by the federal government (Department of Justice, 2005).[20] This is a complex proposition requiring much more than just creating new private-sector partnerships for access to functioning communication infrastructure. To get to this hypothesized end state for the nation with fusion centers, the whole of state and local law enforcement would need to adopt not just public warning but also counterterrorism as an organizational mission. Those efforts would also need to be resourced and fully

[20] DOJ Fusion Center Guidelines (2005) note that fusion centers should create a seamless communication environment and specifically recommend consideration of CAP utilization to enable public warning.

incorporated into a traditionally exclusive federal government intelligence community. At present this seems farfetched. Standing in the way is the problem that not all jurisdictions have a fusion center or an alternative counterterrorism intelligence capability to support the specific information that risk communication principles require. There is also a lack of standardization across the nation in the funding, mission, form, and functioning of the fusion centers that do exist. Even if there were comprehensive nationwide interconnected capability at the local level, there is no clear federal avenue for mandating such a responsibility, providing resource support, or ensuring that it would be uniform. To change this reality would require a financial and political investment so great as to seem unlikely. Moreover, it is doubtful that all states and localities would be willing to assume what could be seen as a federal government responsibility.

IV. SUMMARY ANALYSIS

A. WHERE WE ARE AND HOW WE GOT HERE

Terrorism is unlike any other hazard faced by the American public. It induces fear from unknown threats that lack predictability as to when, where, and how they will occur (Ludman, 2004). It is also the only hazard that can change based upon risk communication with the public (Ward, 2002). As has been shown, efforts to guide the public to take protective measures can lead to changes in the threat, tactics, targeting, or timing. The detailed and accurate information that research recommends is based upon natural hazards that lack the ability to interact with the information being shared. While specificity is equally essential in improving the probability of the public's taking protective action, and thereby saving lives, it is not realistic. As previously noted, terror warnings are only as good as the intelligence that supports them, and detecting hidden plots and defeating surprise attacks will never be perfect (Squires, 2009). Again, information necessary to connect the dots is rarely readily available (Newhouse, 2003), and discreet personal communication would require technology that does not exist. These challenges force the realization that messengers cannot avoid imperfection in warning about terrorism. A perfect public message that is reliable, specific, and actionable is just not possible (Freedman, 2005).

There was and still is a blurred understanding of how best to save American lives from terrorism and address the public's desire to know about future terror threats and government efforts to prevent them. The HSAS has been the only official attempt at a terrorism public-warning system, and it has never aspired to be anything more than a bureaucratic construct partnered with the media. It has taken years to fully understand the unintended consequences that have negatively impacted the public and damaged future homeland security efforts towards efficacy in risk communication. It is a morality tale in

why time should have been taken to study feasibility and approach.[21] Sadly, the research that was conducted prior to implementation was limited to other systems (Ridge, 2009).[22] It took nearly eight years for an official DHS review of the HSAS, and an act of Congress and change in Presidential administration was required for that. Still the HSAS remains in the public realm. Even after the attempted bombing of Northwest Airlines flight #253 from Amsterdam to Detroit on Christmas Day 2009, the airline industry is still set at code orange, as it has been for over three years.

HSAS warnings from DHS, while tangible compared to local messaging, are also plagued by the past. The diversity and complexity of the public coupled with powers of personal perception make warning a tough and demanding task to begin with. Initial missteps and failures make warning even harder. The HSAS has achieved disappointing and unfortunate results. Warnings are now more likely to be tuned out and disregarded, thereby continuing the cycle of unintended consequences (Paul & Park, 2009). The HSAS has generated more jokes and laughter than protective action within its intended audience. The American public has been routinely exposed to images like those displayed in Figure 2, HSAS-related skits on late-night talk shows, and other comics.

Derision has been the public expression of the consensus that the HSAS has failed in meeting its intended purpose; it signals the public's disdain and resistance to its further use (Brigham, 2005). The HSAS levels establishing government policy are laughable to a

[21] Aligning with other nation's policies and practices did not occur in favor of a unilateral approach (Newhouse. 2003). This approach was contrary to research that has found terrorism to be influential in the political formation of coalitions and a low degree of ideological polarization within them (Indridason, 2008).

[22] America is not the only industrialized nation that employs a terrorism warning system or issues terrorism threat advisories to the public. Two of America's closest allies, the United Kingdom and Israel, both have extensive experience with terrorism and terrorism warnings. While not color coded, the UK employs threat levels similar to the HSAS. The key difference between the UK threat levels and the HSAS is that the intended audience is law enforcement, homeland security officials, and practitioners in threatened sectors as determined by intelligence (United Kingdom Cabinet Office, 2009). Israel's approach to terrorism warnings centers on travel or specific geographical areas (Israel National Security Council, 2009). Israeli intelligence is generally accurate enough to identify the city or part of a region that terrorists are targeting (Morag, 2010). As in the UK, much information is kept classified, and efforts are focused on prevention.

public that sees this color-coded chart as childish and lacking leadership. It is telling that the public does not believe that the HSAS makes them safer, and it is questionable whether changes to this system can overcome damaged public perception.

The HSAS task force was a signal that positive change could be possible. Unfortunately, the task force and the report offer little hope that changes will be made that respect research and the scientific understanding of public communication and terrorism. The recommendations offered for communication with the public give a general impression that the authors believe that an advisory system that is truncated to three threat levels, may still be color coded, and that continuing to issue general warnings will be effective. Research suggests otherwise: there is no evidence that in the future detecting a plot, determining a threatened target population, and reaching it in time to warn of a pending attack will be anything more than science fiction. Given this, proceeding with the HSAS and remaining in the public realm requires discussion and understanding of the power of politics. Political motives are the root of the HSAS, what keeps it alive; they represent a challenge that lies in store for homeland security's future regarding public risk communication.

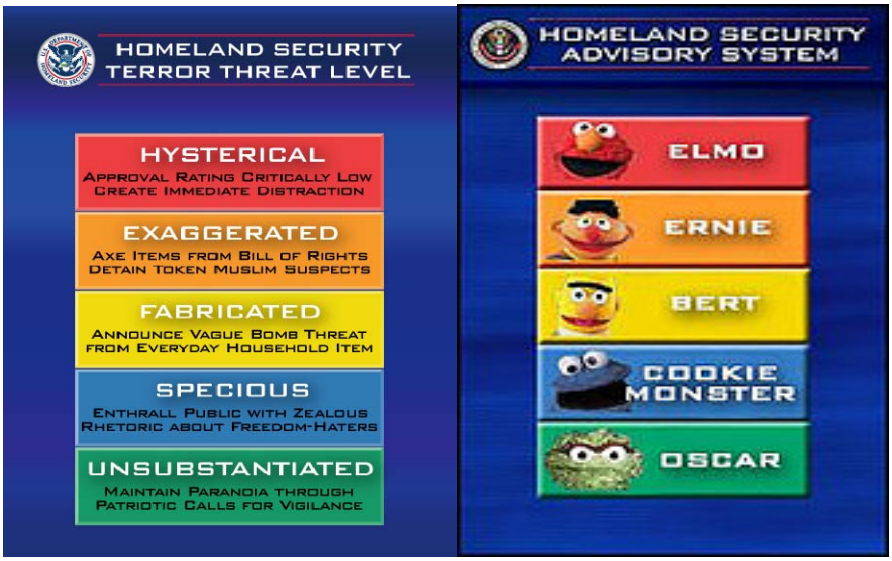

Figure 2. Satirical Graphic Images of the Homeland Security Advisory System (Source: http://images.google.com)

B. ASPECTS OF AMERICAN POLITICS

In early March 2002, the HSAS was being finalized at the White House (Brill, 2003). The cold reality is that during that time even the creators of the color-coded idea knew there were going to be problems with its use in the public realm (Ridge, 2009). The general information that the system was going to convey did not require discussion of related counterterrorism intelligence (Brill, 2003). Threat assessment for implementation of the system amounted to personal perceptions and opinions in the aftermath of 9/11 (Ridge, 2009). Most of the effort was invested in choosing colors and determining the number of levels (Brill, 2003). Even the debate over the initial color level between administration officials was semantic in nature (Brill, 2003).[23] There was pressure to act and timeliness was an issue (Ridge, 2009). President Bush took an oath to protect and serve the public, and the 9/11 attacks occurred on his watch. Having another intelligence or detection failure without the public being warned was untenable (Crawford, 2004). Planning, procedures, quality assurance, efficiency review were all cast aside in the interest of quickly putting a system in place that had political value in addressing public suffering and questioning (Ganor, 2005). Congress was not immune from this pressure either. It was only twelve days after the 9/11 attacks that Congress signed the September 11th Victim Compensation Fund of 2001 (P.L. 107-42) into law (Wolfe, 2003).[24] Six billion dollars was allocated for a program to compensate those who were injured or the families of those who were killed (Wolfe, 2003). This was unprecedented legislation that bailed out the airline industry and addressed the wrongful deaths of the innocent victims. While the administration desired a different approach—tort litigation and funding from the U.S. Treasury—there was no disagreement as to fault and a need for victim compensation (Wolfe, 2003). There simply was no warning, and failed prevention was squarely in the hands of the federal government.

---

[23] At one point, according to Tom Ridge (2009), the President himself was concerned that setting the system at high alert and keeping it there would render the system ineffective.

[24] The Victims of Terrorism Tax Relief Act of 2001 (P.L. 107-134) was also signed into law shortly after the attacks. This act exempted victims from federal income tax for the year of their death and the prior year.

Equally significant to the political pressures following 9/11 was the opportunity it afforded beltway politicians. Around this time, President Bush and key members of his administration were busy framing U.S. counterterrorism efforts as a global war in a different world (Crawford, 2004). The 9/11 attacks were significant enough to change the way that risk was assessed by the United States and how policy was crafted in response to the new risk (Renshon & Suedfeld, 2007). Imminent threats and asymmetrical warfare from stateless actors became the driving force behind the "war on terror" that spanned the globe. America was painted as always being under threat of attack. Fear became institutionalized in U.S. policy (Crawford, 2004). It became a significant part of the American experience, not only for the public but also for politics. Since Hobbes wrote in *Leviathan*, fear has been understood as a powerful tool in getting public support for agendas that claim to keep vulnerable people safe. Fear and the basic public need for government protection allowed for an aggressive domestic political agenda that included massive federal government reorganization, the formation of DHS, and the possibility for the Bush administration and the DHS to ready-fire-aim with the HSAS.

The significance of fear soon became noticeable to those analyzing the support for the administration's new agenda. The fear effect, as it is now known, influenced presidential approval ratings (Willer, 2004). When the HSAS was elevated from yellow to orange, approval ratings also went up (Willer, 2004). In 2005, there were already thirteen documented instances where a terror warning was issued within days of a significant political downturn for the Bush administration with the American public (McDermott & Zimbardo, 2006). People are known to identify with in-groups (Tajfel, 1970) and with terrorism, anxious Americans were identifying more with the president and his counterterrorism efforts. Facing mortality strengthens these ties (Willer, 2004). Reminding people of 9/11 by raising the HSAS threat level increased solidarity with the president (Landau et al., 2004). Sadly, presidential approval was not the darkest of places that politics would take the HSAS. Research has shown that President Bush may have used the HSAS to ensure reelection with voters who would under full advisement have

otherwise voted for John Kerry (Hodler, Loertscher, & Rohner, 2007).[25] Former DHS Director, Tom Ridge, has made statements that would support this notion (Cable News Network, 2009). In an interview with Fran Townsend, the former Bush Homeland Security Advisor and co-chair of the Homeland Security Council's Homeland Security Advisory System Task Force, Tom Ridge is referred to for his confirmation that there was political pressure from others in the Bush administration to raise the HSAS threat level prior to the 2004 election (Cable News Network, 2009). While Townsend no doubt disagreed with Ridge's statements considering her current work on the HSAS, she did confirm that there was discussion about raising the threat level in the sense that it might be a detriment for Bush since people could perceive it as being a political move.[26]

This history demonstrates that politics are potent and fear is a powerful tool, and both them had an ill effect on a communication system that was intended to aid the public, not harm it. Fear regrettably can serve the agendas of not just terrorists but also those elected and sworn to protect against them. The HSAS should never have been used in a manner that supported political agendas or induced fear, lowering its utility to the level of our adversaries. Still, the propaganda following 9/11 was equal mass-media coverage of both the Bush administration's HSAS elevations and Al Qaeda's public addresses from Osama bin Laden (Nacos, Bloch-Elkon, & Shapiro, 2007). Possibly the greatest sign that any remnants of good intentions to warn the public of terrorism had been sacrificed occurred when President Bush himself, after his reelection, credited Osama bin Laden with helping him retain office (Nacos Bloch-Elkon, & Shapiro, 2007). The restraint that President Bush asked of the media in airing bin Laden statements soon after 9/11 were not requested around election time. Fear of terrorism, again, proved

[25] The research was inspired by the 2004 reelection of President George W. Bush and the HSAS elevated threat level that lasted from August 1, 2004, until November 10, 2004. The research intent was to determine whether or not an incumbent could benefit during reelection by issuing distorted terror alerts with rational voters who are aware of the incumbent's incentive and potential to do this. The research showed that it is possible for an incumbent to use terror alerts to manipulate votes for reelection from voters who believe the opposing candidate is better. Related research found that there were significant effects on voting in 2004 from the war on terror and the Iraq war that ultimately favored the incumbent, Bush (Hillygus & Shields, 2005). The researchers found these two issues hard to differentiate since the Bush campaign linked these together, known as Bush Doctrine (Renshon & Suedfeld, 2007).

[26] The Hodler, Loertscher, & Rohner research shows that voter awareness of possible political motivation does not inhibit them from being manipulated into voting against their presuppositions for an incumbent.

valuable. The HSAS was wrapped into politics in a way that perverted fear management and life-saving efforts. This regrettably has come at the expense of the American public that it was intended to serve.[27]

[27] Social and economic impacts have also been found:research has concluded that public fear from heightened alerts can drive down participation in activities and spending (Amegashi & Kutsoati, 2004).

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. RESISTING POLITICAL PRESSURE: DISBANDING THE HSAS

> This system has clearly evolved over time to be used primarily for political ideology, and contains no effective psychological, practical, or even political efficacy.
>
> — Philip G. Zimbardo

President Bush used HSPD-3 and 5 to make it clear that the HSAS was supposed to be an effective way to communicate the risk of terror attacks to the American public. However, what these presidential directives did not do is detail how the HSAS was to distinguish between this audience and government stakeholders. The nature and scale of the 9/11 terror attacks created a political climate that blurred the lines between addressing the fears and safety of the American public and sharing vital counterterrorism intelligence with government stakeholders. Yigal Pressler, former advisor to the Israeli Prime Minister on counterterrorism, once stated that most decisions are made immediately following an attack, only to find difficulty months later when they are tested with reality (Ganor, 2005). The reality test for the HSAS is that ultimately no authority invested in prevention is ever going to aid an adversary, hidden within the general population, with specific intelligence.

What is left for HSAS warnings is pursuing ambiguity or no public warning at all. Debate on these options is encouraged and believed to be again necessary and worthwhile. It is unfortunate that the HSAS Task Force Report and Recommendations was not the vehicle for this. The report's recommendations, specific to the general public, keep the HSAS as a public communication tool. Doing so will have to contend with the past and how the public's perception has been shaped. Changing the HSAS will face the significant challenge of gaining and regaining the public ear. The people and society in general have not looked favorably on the HSAS. Generalized warnings and published criticisms of the HSAS have had a negative impact on people's understanding of the HSAS, on the level of trust in the system, and on its effectiveness in directing public action. For a leader to proceed with this in mind and an understanding of trust

relationships is counterproductive. Damaged credibility, such as what is presently at hand with the HSAS, impedes messenger effectiveness. Warnings can fall flat in these instances and opportunities to influence the threatened public into taking protective action can be lost.

Resigning ourselves to providing simplified overviews of threat environment will sustain a system that manufactures unintended consequences. These problems have locked the HSAS in a holding pattern that has lasted since 2006, making it increasingly irrelevant. Considering these problems, the notion of no communication should be understood as closing this chapter of America's homeland security history. When considering whether or not it is politically tenable for the president and the DHS to not issue terrorism threat advisories to the American public, it is important to understand that, even during the time that the HSAS was created and established, there were individuals within the Bush administration and the DHS who believed that terror warnings should be outside of the public realm (Fenzel, 2008). The argument for this approach placed prevention of a terrorist attack over warning the public. Counterterrorism intelligence for this end would be controlled and limited in distribution to only those with a need to know and who are stakeholders in interdicting the terrorists and disrupting their plot. It is time to return to government's responsibilities to protect its people. Saving a life from terrorism is done best by making sure that a warning is not necessary. Terrorism prevention must be the priority and means for doing that.

Consistency with a flawed approach is simply perpetuation of a problematic system that has been bastardized by politics and become stigmatized and marginalized. The intrinsic qualities of a terror warning which could help save lives has never been achieved because of this flawed approach and never will. The HSAS should be retired and its communication process disbanded and reorganized in a manner that excludes the public. As world-renowned psychologist and researcher Dr. Philip Zimbardo (2009) states, "The terror alert system as practiced in the United States is less than worthless, and needs to be thoroughly revised. That revision must be based on our understanding of effective emergency warning systems and the psychological analysis of how best to motivate citizens for impending dangers facing them."

The concept of terrorism threat advisories should be removed from the public realm entirely. Advisories should remain a private prevention-based homeland security function. The American public does not need to be intimately involved in the intelligence community to the detriment of prevention efforts and the public's psychological well-being. Any perceived political necessity to provide terrorism threat advisories to the public can be satisfied with controlled and limited distribution within law enforcement and the intelligence community. There simply is no better news than that of a prevented attack. This positive result of counterterrorism is the righteous way to pursue public approval and political ambitions.

B. A NEW DIRECTION

> Terrorism is about one thing: Psychology. It is the psychology of fear.
>
> — Philip G. Zimbardo

Recommending policy that would terminate the HSAS is done with the understanding that history is known for repeating itself. It is unrealistic to consider prevention perfected, and closure for the HSAS should not be considered a portrayal of an American future that is free from terror attacks. The significantly heavy burden placed on counterterrorism intelligence and the intelligence community (IC) to defeat surprise and prevent terrorism is no less today than it was when the HSAS was created. Future attacks on American soil must be factored into the development of new homeland security policy regarding public terrorism risk communication. Efforts thus far with the HSAS have not immunized Americans from the perils of politics or the psychology of terrorism. America is not cultured to understand that prevention is not absolute, and people are prone to losing sight of the threat of terrorism when not educated. A 2009 Gallup Poll (Morales, 2009) showed a decline in American's level of concern for terrorism. Only one percent listed terrorism as the most important problem that America faces and 73 percent claimed a fair or great deal of confidence in the U.S. government's ability to protect citizens from future terrorist attacks. At the same time, other research has shown that only one in three Americans trusts government warnings, and three quarters of Americans do not believe that government has explained how to prepare for

terrorism (Breckenridge, 2009). While just a snapshot in time, these figures are representative of the possible public perceptions that U.S. policy could face when another successful attack occurs on U.S. soil, killing Americans. Prevention is not absolute, and the public should be concerned and encouraged to participate and prepare for the realistic eventuality of future attacks. Avoiding the same significant problems in politics and public accountability that came with 9/11 should be the focus of policy development.

The impacts of the 9/11 attacks are rightfully enormous. They continue to demand that government communicate with the public regarding terrorism and to improve on the public service that has been provided thus far. However, the time is right for this to happen in a manner that is consistent with research-based understandings of psychosocial science that have bearing on our success in reaching the threatened public and achieving the recommended response. To right past wrongs, we must pause to understand the social psychology implications of what we are trying to achieve (Zimbardo & Kluger, 2003; Bongar, 2007). The scientific pioneers who separated the psychology of terrorism risk communication from other hazards through mental health research, continued questioning, and testing have moved our understandings into an established field of study (Flynn, 2004; Bongar, 2007). Because of this, we should never again ignore how the psychology of fear impacts the interconnections between government, the public, and terrorists when we try to warn. The time is right for government to begin taking the terror out of terrorism through fear management education that addresses the psychological underpinnings of public perception and action (Breckenridge & Zimbardo, 2007). Simply improving HSAS advisories and clarifying citizen guidance about a revision to the system will not be sufficient to restore public trust and confidence in government homeland security efforts (Breckenridge, 2009). A new approach is now necessary. Research data still shows a public that lacks confidence that homeland security professionals and government will be open and tell the truth (Breckenridge, 2009). Overcoming this requires public education on the issue of terrorism and outreach for hazard-specific preparedness (Ganor, 2005). Engaging the public in efforts to be informed and active in countering terrorism and protecting themselves and others is key

to our future homeland security efforts (Zimbardo, 2009). Giving the public strength from understanding and knowledge will help combat fear and distrust.

Efforts toward establishing new policy should be encouraged, noting examples from other nations, such as Israel. Israel is one example of a national approach being directed at removing the psychology of fear from terrorism. (Homeland Security Institute, 2009). Founded on a civil defense law from 1951, Israelis are cultured to prepare for threats of terrorism and successful attacks (Israeli Home Front Command, 2010). Preparedness begins with education from kindergarten to completion of the twelfth grade (Homeland Security Institute, 2009). In conjunction with the Ministry of Education, classes continually expose children and young adults to the reality of the threat and how to cope (Israeli Home Front Command, 2010). Education is also supported by an annual national drill required for all of Israel's educational institutions (Israeli Home Front Command, 2010). These measures are indicative of a more frequent exposure to terrorist attacks than is the United States at present. However, with an unknown future, this example can serve as a starting point for valuable further research. Sound and just approaches to public service and risk communication will be better obtained before the threat environment in the United States changes.

Fortunately, post-9/11 preparedness initiatives afford policy makers a place to start. Public outreach continues to be a priority, and DHS has even published guidelines for this practice (DHS, 2007b). Initiatives such as Citizen Corps have led to valuable research findings to help understand why people do not prepare and to recommend education for changing behavior (DHS, 2006).[28] Add to this the National Strategy for Homeland Security (DHS, 2007c), which encourages personal responsibility for surviving an attack and providing for basic needs in the aftermath, and it becomes more apparent that it is possible for policy to grow towards future social conditioning that

[28] The Citizen Corp Personal Behavior Change Model for Disaster Preparedness (DHS, 2006) asserts that individuals decide not to prepare for disasters because they do not perceive a threat or susceptibility to a threat, or they perceive a threat or susceptibility but perceive barriers to preparedness activities. The model also recommends community outreach through a risk-based preparedness program that would provide educational messages about the threats, personal vulnerability, and related preparedness activities and mitigation measures. The model recommends that this be followed by efficacy messaging and behavior maintenance and reinforcement.

better aids people to endure terrorism (Ripley, 2008). Research has shown that readiness and willingness to comply with government directions for protective action is greater with citizens who view their role as a duty (Breckenridge, 2009). Education towards duty and involvement is much more substantial than websites, volunteer programs, and periodic training courses. In order to help a public that has been shown to have a strong desire for involvement in its own defense but feels that the government has not done enough for public participation, we must do more to listen to the opinions of the public and to provide them with opportunities to contribute (Breckenridge, 2009).[29] Only through partnership with the public that affords it opportunities to participate will we be able to reach a point where the public is confident that homeland security is competent and trustworthy (Breckenridge, 2009).

Helpful and relevant information must be woven into school curricula, and knowledge must be cultivated in the public through innovative ways of preparing for terrorism similar to other mental and physical health practices. Transformation will be defined by leaders who want to be agents for a necessary change process that moves U.S. policy beyond the HSAS concept. To be a more resilient nation, capable of better withstanding the aims of terrorists and misaligned political ambitions, policy must guide the United States to a healthier and more realistic education strategy.[30] Planning strategically to better achieve what the HSAS has not can be an effective way to solve problems and rebuild public trust (Bach, 2010). The HSAS is an already-written story. The sequel should be the narrative explaining how the American public will be told who might attack and how, what can be done to help prevent an attack, and what to do after an attack because there is a probability of such an occurrence (Ripley, 2008). Benjamin Netanyahu, Israeli Prime Minister, once stated that terrorism education in school curricula can assist government in creating a citizenry that can live with terrorism and not

[29] The American Perceptions Study is a national study of 4,000 American adults that began in November 2008 (Breckenridge, 2009).

[30] U.S. military information operations, as highlighted in past Quadrennial Defense Review Reports, have been recommended for enhancement through education of information operations forces in psychology and sociology. Success for this mission area has been argued to be possible, in part, through a complete change in culture, altering foundational beliefs about educational understanding of the sciences relating to information operations (Durkin et al., 2007).

succumb to its aims (Ganor, 2005). Trusting government is the foundation for public risk communication (Ripley, 2008), and in the case of terrorism in America, this should be developed and sustained from public education. A strong and resilient public makes for a better American future.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amegashie, A. J., & Kutsoati, E. (2004). Terror alerts and beliefs about terrorism. http://www.uoguelph.ca/~jamegash/Terrorism_Beliefs.pdf (accessed August 19, 2009).

Arizona Department of Public Safety. (2009). Arizona Counter Terrorism Information Center: Mission. http://cid.dps.state.az.us (accessed March 2, 2009).

Association of State and Territorial Health Officials. (2002). Communication in risk situations: Responding to the communication challenges posed by bioterrorism and emerging infectious diseases. http://www.astho.org/docs/productions/workbook.htm (accessed February 24, 2009).

Australian National Counter-Terrorism Committee. (2008). National counter-terrorism plan. http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(3273BD3F76A7A5DEDAE36942A54D7D90)~National+Counter-Terrorism+Plan+-+Alert+System+Changes+October+2008+PDF.PDF/$file/National+Counter-Terrorism+Plan+-+Alert+System+Changes+October+2008+PDF.PDF (accessed August 19, 2009).

Australian Government National Security. (2009a). National Counter-Terrorism Alert System Fact Sheet. http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~Alert+System+-+Australian+Government+Fact+Sheet+Word+Version+FINAL.pdf/$file/Alert+System+-+Australian+Government+Fact+Sheet+Word+Version+FINAL.pdf (accessed August 19, 2009).

Australian Government National Security. (2009b). National Counter-Terrorism Alert System. http://www.ag.gov.au/agd/WWW/NationalSecurity.nsf/Page/Information_for_Individuals_National_Security_Alert_System_National_Counter-Terrorism_Alert_System (accessed March 17, 2009).

Bach, R. (2010). Lecture: Strategic planning and budgeting for homeland security. Naval Postgraduate School. Monterey, CA.

Bachmann, R. (2006). Trust and/or power: Towards a sociological theory of organizational relationships. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research*, 393–406. Northampton, MA: Edward Elgar.

Banerjee, S., Bowie, N. E., & Pavone, C. (2006). An ethical analysis of the trust relationship. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research*, 303–16. Northampton, MA: Edward Elgar.

Bettenhausen, M. (2008). Moving beyond the first five years: Evolving the office of intelligence and analysis to better serve state, local, and tribal needs. Testimony before the House Homeland Security Committee Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. Washington, D.C., April 24, 2008.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory. In M. Connor & P. Norman (Eds.), *Predicting health behavior*, 95–120. Buckingham, U.K.: Open University Press.

Bongar, B. (2007). The psychology of terrorism. In B. Bonger, L. Beutler, J. Breckenridge, & P. G. Zimbardo (Eds.), *The psychology of terrorism*, 3–12. New York: Oxford University Press.

Breckenridge, J. (2009). Letter to Jeff Karonis at the U.S. Department of Homeland Security regarding the Homeland Security Advisory System. Stanford, CA.

Breckenridge, J. (2010). Lecture: The psychology of fear management and terrorism. Naval Postgraduate School. Monterey, CA.

Breckenridge, J., & Zimbardo, P. G. (2007). The strategy of terrorism and the psychology of mass-mediated fear. In B. Bonger, L. Beutler, J. Breckenridge, & P. G. Zimbardo (Eds.), *The psychology of terrorism*, 116–33. New York: Oxford University Press.

Brigham, J. (2005). Anti-anti terror: Color coding and the joke of homeland security. *New Political Science* 27(4): 481–96.

Brill, S. (2003). *After: How America confronted the September 12 era*. New York: Simon & Schuster.

Bush, G. W. (2002). Homeland Security Presidential Directive 3. http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html (accessed January 17, 2009).

Bush, G. W. (2003). Homeland Security Presidential Directive 5. http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (January 17, 2009).

Bush, G. W. (2006). Executive Order: Public Alert and Warning System. http://www.whitehouse.gov/news/releases/2006/06/print/20060626.html (accessed January 17, 2009).

Cable News Network (2009). Frances Townsend: Tom Ridge has it wrong. American Morning—amFIX. http://amfix.blogs.cnn.com/2009/08/21/frances-townsend-tom-ridge-has-it-wrong (accessed August 24, 2009).

Corman, S. R., Goodall, B., & Trethewey, A. (2007). A twenty-first century model for communication in the global war of ideas. Report #0701. Tempe: AZ: Consortium for Strategic Communication, Arizona State University.

Covello, V. T. (1998). Risk perception and communication. *Proceedings of the North American Conference on Pesticide Spray Drift Management*, March 29–April 1, 1998. Portland, ME: University of Maine Cooperative Extension, 161–186.

Covello, V. T., McCallum, D. B., & Pavlova, M. T. (2004). *Effective risk communication: The role and responsibility of government and nongovernment organizations. Vol. 4, Contemporary issues in risk communication*. New York: Plenum Publishing Corporation.

Cox, C. (2004). Testimony before the United States Select Committee on Homeland Security Hearing: Homeland Security Advisory System. http://bulk.resource.org/gpo.gov/hearings/108h/22132.pdf (accessed January 23, 2009).

Crawford, N. C. (2004). The road to global empire: The logic of U.S. foreign policy after 9/11. *Foreign Policy Research Institute* (Fall 2004): 685–703.

Czarnecki, E. (2008). Private sector roles are expanding for public alerts and warnings. https://www.bia.com/data_perspective_022707.asp (accessed February 19, 2009).

Dahl, E. J. (2005). Warning of terror: Explaining the failure of intelligence against terrorism. *Journal of Strategic Studies* 28 (1): 31–55.

Davis, D., & Silver, B. (2004). The threat of terrorism, presidential approval, and the 2004 election. Prepared for delivery at the annual meeting of the American Political Science Association, September 2–5, 2004, Chicago, Illinois.

DeYoung, K. (2006). In Arizona, officials share data the old-fashioned way. *Washington Post.* http://www.washingtonpost.com/wp-dyn/content/article/2006/08/08/AR2006080801007.html (accessed February 20, 2009).

Dirks, K. T. (2006). Three fundamental questions regarding trust in leaders. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research*, 15–27. Northampton, MA: Edward Elgar.

Disaster Response, Recovery, and Mitigation Enhancement Act of 2009. (2009). H.R. 3377. Eleventh Congress, First Session.

Durkin, M. F., Franz, T. P., Mills, R. F., Raines, R. A., & Williams, P. D. (2007). Defining information operations forces: What do we need? *Air & Space Power Journal* (Summer 2007).

Evening Standard. (2007). MI5 launches instant terror alerts by email. http://www.thisislondon.co.uk/news/article-23380584-details/MI5+launches+instant+terror+alerts+by+email/article.do (accessed February 17, 2009).

Federal Communications Commission. (2008). FCC Consumer Facts: The Emergency Alert System (EAS). http://www.fcc.gov/cgb/consumerfacts/eas.html (accessed February 9, 2009).

Federal Emergency Management Agency. (2008). Integrated Public Alert and Warning System (IPAWS). http://www.fema.gov/emergency/ipaws (accessed March 7, 2010).

Fenzel, J. (2008). Public warning. http://johnfenzel.typepad.com/john_fenzels_blog/public_warning (accessed February 17, 2009).

Flynn, B. W. (2004). Commentary on "A national longitudinal study of the psychological consequences of the September 11, 2001 terrorist attacks: Reactions, impairment, and help-seeking. Can we influence the trajectory of psychological consequences to terrorism?" *Psychiatry* 67: 164–66.

Forsyth, W. A. (2005). State and local intelligence fusion centers: An evaluative approach in modeling a state fusion center. Master's thesis, Naval Postgraduate School.

Freedman, L. (2005). The politics of warning: terrorism and risk communication. *Intelligence and National Security* 20(3): 379–418.

Gallup Organization. (2004). Government trust little changed from last year: But highly related to presidential preference in specific areas. http://www.gallup.com/poll/14026/Government-Trust-Little-Changed-From-Last-Year.aspx (accessed August 19, 2009).

Ganor, B. (2005). *The counter-terrorism puzzle: a guide for decision makers.* International Institute for Counter-Terrorism, Interdisciplinary Center Herzliya. London, U.K.: Transaction Publishers.

General Accounting Office. (2004a). Communication protocols and risk communication principles can assist in refining the advisory system. www.gao.gov/cgi-bin/getrpt?GAO-04-682 (accessed January 23, 2009).

General Accounting Office. (2004b). Homeland security advisory system: preliminary observations regarding threat level increases from yellow to orange. http://www.gao.gov/products/GAO-04-453R (accessed January 23, 2009).

General Accounting Office. (2007). Emergency preparedness: current emergency alert system has limitations, and development of new integrated system will be challenging. GAO-07-411.

Gomez, A. (2009). Cities rethink high-tech alert systems. *USA Today*. http://www.usatoday.com/news/nation/2009-07-06-ealerts_N.htm (accessed August 19, 2009).

GovTrack.us. H.R. 3266—108th Congress. (2003). Faster and smarter funding for First Responders Act of 2004. http://www.govtrack.us/congress/bill.xpd?bill=h108-3266 (accessed December 20, 2008).

GovTrack.us. H.R. 2101—109th Congress. (2005). To amend the Homeland Security Act of 2002 to direct the Secretary of Homeland Security. http://www.govtrack.us/congress/bill.xpd?bill=h109-2101 (accessed December 20, 2008).

GovTrack.us. H.R. 5001—109th Congress (2006). Homeland Security Information Sharing Enhancement Act of 2006. http://www.govtrack.us/congress/bill.xpd?bill=h109-5001 (accessed December 20, 2008).

Hillygus, S. D., & Shields, T. G. (2005). Moral issues and voter decision making in the 2004 presidential election. *PS: Political Science and Politics* 38(2): 201–9.

Hobbes, T. (1904). *Leviathan: Or the matter, forme and power of a commonwealth, ecclesiasticall and civill*. Edited by Michael Oakeshott. Oxford: Basil Blackwell, 1946.

Hodler, R., Loertscher, S., & Rohner, D. (2007). False alarm? Terror alerts and reelection. Department of Economics – Working Papers Series 995, Melbourne, Australia: University of Melbourne.

Homeland Security Advisory Council. (2009). Homeland security advisory system task force report and recommendations. http://www.dhs.gov/xlibrary/assets/hsac_final_report_09_15_09.pdf (accessed September 16, 2009).

Homeland Security Institute. (2009). Public role and engagement in counterterrorism efforts: Implications of Israeli practices for the US. http://www.homelandsecurity.org/hsireports/Public_Role_in_CT_Israeli_Practices_Task_08-22.pdf (accessed January 9, 2010).

Hsu, S. S. (2006). Bush orders update of emergency alert system. *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/26/AR2006062601304.html (accessed February 10, 2009).

Indridason, I. H. (2008). Does terrorism influence domestic politics? *Journal of Peace Research* 45: 241–259.

Israel National Security Council. (2009). Activities of the counter-terrorism bureau. http://www.nsc.gov.il/NSCWeb/TemplatesEnglish/CounterTerrorismActivitiesEN.aspx (accessed February 24, 2009).

Israeli Home Front Command. (2010). Training the public: Source of home front command's authority. http://www.oref.org.il/79-1611-en/PAKAR.aspx (accessed January 9, 2010).

Johnson, D., & Risen, J. (2003). New signs of terror not evident. *New York Times*. http://www.nytimes.com/2003/04/06/international/worldspecial/06SECU.html (accessed August 19, 2009).

Jones, J. M. (2003). Fear of terrorism increases amidst latest warning. Gallup, Inc. http://www.gallup.com/poll/7792/Fear-Terrorism-Increases-Amidst-Latest-Warning.aspx (accessed August 20, 2009).

Jones-Hard, S. G. (2004). Bio-terrorism: Steps to effective public health risk communication and fear management. Master's thesis, Naval Postgraduate School.

Kahneman, D. (1979). Prospect theory: An analysis of decision under risk. *Econometrica* 47(2): 263–92.

Khalsa, S. K. (2004). Terrorism forecasting: A web-based methodology. Center for Strategic Intelligence Research, Joint Military Intelligence College. Washington, D.C.

Korn, M. (2009). Color-code terror alerts remain in force. *Dallas Morning News*. http://www.dallasnews.com/sharedcontent/dws/news/nation/stories/DN-wonderbox_25nat.ART.State.Edition1.4c0f244.html (accessed August 19, 2009).

Kramer, R. M. (2006). Trust as situated cognition: An ecological perspective on trust decisions. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research*, 68–82. Northampton, MA: Edward Elgar.

Landau, Mark, Solomon, S., Greenberg, J., Cohen, F., Pyszczynski, T., Arndt, J., Miller, C. H., Ogilvie, D. M., & Cook, A. (2004). Deliver us from evil: The effects of mortality salience and reminders of 9/11 on support for President George W. Bush. *Personality and Social Psychology Bulletin* 30(9): 1136–50.

Lipowicz, A. (2008). FEMA adopts open standards. *Federal Computer Week*. http://fcw.com/Articles/2008/09/05/FEMA-adopts-open-standards.aspx (accessed February 19, 2009).

Ludman, B. L. (2004). Israel leads in making terror warnings effective. *Israel News Agency*. http://www.israelnewsagency.com/israelterrorismwarnings29931.html (accessed February 17, 2009).

McCarter, M. (2009). Napolitano orders review of color-coded alerts. http://www.hstoday.us/content/view/9366/128 (accessed August 19, 2009).

McDermott, R., & Zimbardo, P. G. (2006). The psychology of terrorist alarms. In B. Bonger, L. Beutler, J. Breckenridge, & P. G. Zimbardo, *The psychology of terrorism*, 357–70. New York: Oxford University Press.

Moore, D. (2003). Majority of Americans not ready for terrorist attack. Gallup, Inc. http://www.gallup.com/poll/7936/Majority-Americans-Ready-Terrorist-Attack.aspx (accessed August 20, 2009).

Moore, D. (2004). Government trust little changed from last year. Gallup, Inc. http://www.gallup.com/poll/14026/Government-Trust-Little-Changed-From-Last-Year.aspx (accessed August 20, 2009).

Moore, L. K. (2009). CRS Report for Congress: The Emergency Alert System (EAS) and All-Hazard Warnings. http://www.fas.org/sgp/crs/homesec/RL32527.pdf (accessed August 31, 2009).

Morag, N. (2010). Homeland security and intelligence: Does the new structure work? In Keith Logan (Ed.), *Homeland security and intelligence*. Westport, CT: Praeger.

Morales, L. (2009). Americans' worry about terrorism nears 5-year low. Gallup, Inc. http://www.gallup.com/poll/121379/americans-worry-terrorism-nears-year-low.aspx (accessed August 20, 2009).

Nacos, B. L., Bloch-Elkon, Y., & Shapiro, R. Y. (2007). Post-9/11 terrorism threats, news coverage and public perceptions in the United States. *International Journal of Conflict and Violence* 1(2): 105–26.

National Center for Missing & Exploited Children. (2008). Amber Alert Program. http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=991 (accessed February 9, 2009).

National Commission on Terrorist Attacks upon the United States. (2004). 9/11 Commission Report. http://www.9-11commission.gov/report (accessed February 24, 2009).

Nenneman, M. (2008). An examination of state and local fusion centers and data collection methods. Master's thesis, Naval Postgraduate School.

Newhouse, J. (2003). *Imperial America: The Bush assault on the world order*. New York: Knopf.

Newport, F. (2002). U.S. goes to higher alert status. CNN Breaking News, Cable News Network LP, September 10, 2002. http://edition.cnn.com/TRANSCRIPTS/0209/10/bn.06.html (accessed August 20, 2009).

Osborne, D. (2009). Arizona counter terrorism information center: where analysis is central. http://www.lawofficer.com/news-and-articles/columns/Osborne/actic.html (accessed February 20, 2009).

Parker, L. J. (2005). Agroterrorism risk communication: Challenges and implications for communicators. Master's thesis, Naval Postgraduate School.

Partnership for Public Warning. (2004). Protecting America's communities: An introduction to public alert and warning. http://tap.gallaudet.edu/Emergency/Nov05Conference/EmergencyReports/handbook.pdf (accessed February 23, 2009).

Paul, J., & Park, S. (2009). With the best of intentions: The color coded homeland security advisory system and the law of unintended consequences. *Research and Practice in Social Sciences* 4(2): 1–13.

Pinker, E. J. (2007). An analysis of short-term responses to threats of terrorism. *Management Science* 53(6): 865–80.

Reese, S. (2008). Homeland security advisory system: possible issues for congressional oversight. Congressional Research Service. http://assets.opencrs.com/rpts/RL32023_20080129.pdf (accessed January 23, 2009).

Renshon, S.A., & Suedfeld, P. (2007). *Understanding the Bush doctrine: Psychology and strategy in an age of terrorism.* New York: Routledge.

Ridge, T. (2009). *The test of our times: America under siege and how we can be safe again.* New York: Thomas Dunne Books.

Ripley, A. (2008). *The unthinkable: Who survives when disaster strikes and why*. New York: Crown.

Smelser, N. J. (2007). *The faces of terrorism: Social and psychological dimensions.* Princeton, NJ: Princeton University Press.

Squires, K. D. (2009). Critical accountability: preventing and interdicting terrorist activity in the U.S. by effectively utilizing state and local law enforcement. Master's thesis, Naval Postgraduate School.

Sternstein, A. (2009). Hill demands FEMA quickly upgrade aging public warning system. Nextgov. http://www.nextgov.com/nextgov/ng_20091001_6373.php?oref=topnews (accessed October 5, 2009).

Stine, R. J. (2008). Will the EAS house be put in order? Radio World. http://www.rwonline.com/article/64698 (accessed February 19, 2009).

Tajfel, H. (1970). Experiments in intergroup discrimination. *Scientific American* 223: 96–102.

Transportation Security Administration. (2009). Make your trip better using 3-1-1. http://www.tsa.gov/311/index.shtm (accessed February 25, 2009).

Treves, A., & Palmqvist, P. (2007). Hominin interactions with mammalian carnivores. In S. Gursky & K. A. I. Nekaris, *Primate anti-predator strategies*, 355–81. New York: Springer Science+Business Media.

United Kingdom Cabinet Office. (2009). Threat levels: The system to assess the threat from international terrorism. http://www.cabinetoffice.gov.uk/security_and_intelligence/community/threat_levels.aspx (accessed August 19, 2009).

United Kingdom Security Service. (2009). The UK's threat level system. http://www.mi5.gov.uk/output/the-uks-threat-level-system.html (accessed February 17, 2009).

United States Conference of Mayors. (2003). Survey on cities' direct homeland security cost increases related to war/high threat alert. http://www.usmayors.org/pressreleases/documents/survey_032703.pdf (accessed January 23, 2009).

United States Congress. (2003). Senate Governmental Affairs Committee, State and Local Homeland Security Challenges, unprinted hearing of 108th Cong., 1st sess., May 1, 2003.

United States Congress. (2007a). H.R. 1: Implementing Recommendations of the 9/11 Commission Act of 2007. http://thomas.loc.gov/cgi-bin/bdquery/z?d110:H.R.1:@@@L&summ2=m&#major%20actions (accessed September 16, 2009).

United States Congress. (2007b). Public Law 110-53: Implementing Recommendations of the 9/11 Commission Act of 2007. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.pdf (accessed March 5, 2010).

United States Congress. (2009a). H.R. 2892, S. 1298: Department of Homeland Security Appropriations Act, 2010. http://thomas.loc.gov/cgi-bin/cpquery/R?cp111:FLD010:@1(sr031) (accessed September 17, 2009).

United States Congress. (2009b). H.R. 6947: Department of Homeland Security Appropriations Act, 2009. http://www.thomas.gov/cgi-bin/query/z?c110:H.R.6947 (accessed February 19, 2009).

United States Department of Homeland Security. (2003). TOPOFF 2 After action summary report for public release. www.dhs.gov/xlibrary/assets/T2_Report_Final_Public.doc (accessed December 20, 2008).

United States Department of Homeland Security. (2006). Citizen Corps personal behavior change model for disaster preparedness. http://www.citizencorps.gov/pdf/citizen_prep_review_issue_4.pdf (accessed January 9, 2010).

United States Department of Homeland Security. (2007a). TOPOFF 4 full-scale exercise (FSE) After action quick look report. http://www.fema.gov/pdf/media/2008/t4_after%20action_report.pdf (accessed December 20, 2008).

United States Department of Homeland Security. (2007b). National preparedness guidelines. http://www.dhs.gov/files/publications/gc_1189788256647.shtm (accessed January 9, 2010).

United States Department of Homeland Security. (2007c). National strategy for homeland security. http://www.dhs.gov/xabout/history/gc_1193938363680.shtm (accessed January 9, 2010).

United States Department of Homeland Security. (2008a). The TOPOFF 4 full-scale exercise. http://www.dhs.gov/xprepresp/training/gc_1179430526487.shtm (accessed December 20, 2008).

United States Department of Homeland Security. (2008b). Chronology of changes to the Homeland Security Advisory System. http://www.dhs.gov/xabout/history/editorial_0844.shtm (accessed January 23, 2009).

United States Department of Homeland Security. (2008c). Ready.gov. http://www.ready.gov (accessed January 23, 2009).

United States Department of Homeland Security. (2008d). TOPOFF: Exercising national preparedness. http://www.dhs.gov/xprepresp/training/gc_1179350946764.shtm (accessed December 20, 2008).

United States Department of Justice. (2005). Fusion center guidelines: Developing and sharing information and intelligence in a new era. http://www.it.ojp.gov/documents/fusion_center_executive_summary.pdf (accessed March 2, 2009).

United States Department of State. (2002). TOPOFF (Top Officials). http://www.state.gov/s/ct/rls/fs/2002/12129.htm (accessed December 20, 2008).

United States House of Representatives, Subcommittee on Economic Development, Public Buildings, and Emergency Management. (2008a). Statement of the Honorable James L. Oberstar, Hearing on "Assuring public alert systems work to warn American citizens of natural and terrorist disasters." http://www.iaem.com/publications/News/documents/Oberstar_000.pdf (accessed March 7, 2010).

United States House of Representatives, Committee on Transportation and Infrastructure Oversight and Investigations. (2008b). Hearing on assuring public alert systems work to warn American citizens of natural and terrorist disasters. http://www.iaem.com/publications/News/documents/Summary060408.pdf (accessed February 19, 2009).

United States Senate, Committee on Commerce, Science, and Transportation. (2005). Senate Commerce Committee approves WARN Act. http://commerce.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=844294e7-7c2a-496c-b8e4-a1656bfac14f&Month=10&Year=2005 (accessed December 20, 2008).

Ward, P. L. (2002). Delivering clear and effective warnings: applying lessons from natural hazards to terrorism. American Geophysical Union. http://www.agu.org/sci_soc/policy/ward.html (accessed February 17, 2009).

Washington Post. (2004). State of Michigan 2004 election results. http://www.washingtonpost.com/wp-srv/elections/2004/mi (accessed September 30, 2009).

Weiss, R. (2005). Scientists complete genetic map of the chimpanzee. *Washington Post.* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/31/AR2005083102278.html (accessed August 27, 2009).

White House Press Secretary. (2003). Fact sheet: Strengthening intelligence to better protect America. http://www.state.gov/s/ct/rls/fs/2003/17007.htm (accessed March 2, 2009).

Willer, R. (2004). The effects of government-issued terror warnings on presidential approval ratings. http://www.uiowa.edu/~grpproc/crisp/crisp.10.1.html (accessed February 17, 2009).

Winters, J. (2002). Why we fear the unknown. *Psychology Today.* http://www.psychologytoday.com/articles/200305/why-we-fear-the-unknown (accessed January 5, 2010).

Wolfe, A. M. (2003). Homeland security: 9/11 victim relief funds. Congressional Research Service, Library of Congress. RL31716. Updated August 24, 2004.

Zimbardo, P. G. (2003). The political psychology of terrorist alarms. American Psychological Association. http://www.apa.org/about/division/terrorism.html (accessed February 17, 2009).

Zimbardo, P. G. (2009). Letter to Jeff Karonis at the U.S. Department of Homeland Security regarding the Homeland Security Advisory System. Stanford, CA. July 26, 2009.

Zimbardo, P. G., & Kluger, B. (2003). Phantom menace: Is Washington terrorizing us more than al Qaeda? *Psychology Today* 3: 34–36.

Zuberbuhler, K. (2007). Predation and primate cognitive evolution. In S. Gursky & K. A. I. Nekaris (Eds.), *Primate anti-predator strategies*, 3–26. New York: Springer Science+Business Media.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Christopher Bellavita
   Naval Postgraduate School
   Monterey, California

4. Lauren F. Wollman
   Naval Postgraduate School
   Monterey, California

5. Ellen M. Gordon
   Naval Postgraduate School
   Monterey, California